Eric Puchner

IT-riskienhallinta Yritys X:ssä

Metropolia Ammattikorkeakoulu
Tradenomi, ylempi ammattikorkeakoulututkinto
Yrittäjyys ja liiketoimintaosaaminen
Opinnäytetyö
11/2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Eric Puchner IT-riskienhallinta Yritys X:ssä 48 sivua + 6 liitettä 2.11.2015
Tutkinto	Tradenomi, ylempi ammattikorkeakoulututkinto
Koulutusohjelma	Yrittäjyys ja liiketoimintaosaaminen
Suuntautumisvaihtoehto	
Ohjaaja(t)	lehtori Erkki Sairanen

Tutkimustehtävänä oli selvittää, kuinka tutkimuskohteeksi valittu yritys voi kehittää IT-riskienhallintaa ja minkälaisia riskejä tutkimuksessa ilmenee. Tutkimuskohteeksi valittiin Yritys X, joka on rekrytointiin ja soveltuvuusarviointiin erikoistunut yritys. Kehittämistehtävän tuotoksena yritykselle luotiin riskienhallintasuunnitelmia ja käytännöt, joilla riskejä arvioidaan ja niiden toteutumista seurataan.

Tutkimus oli toimintatutkimus, jossa riskejä arvioitiin määrällisin tutkimusmenetelmin. Kehittämistehtävässä käytetty teoria koostuu strategisesta IT-riskienhallinnasta ja riskienhallinnan käytännön toimenpiteiden teorioista ja tätä tutkimustehtävää tukevasta muutosjohtamisen teoriasta.

Lähtötilanteen analysoinnin perusteella tehtiin kattava riskilista, jossa on määritelty paikallisesti vaikuttavat IT-riskit. Riskit luokiteltiin ryhmiin, jolloin niitä on helpompi arvioida kokonaisuuksina. Yrityksen johdon päätöksenteko helpottuu, kun riskeihin varautumisesta voidaan yksittäisten riskien sijaan päättää ryhmittäin. Riskit arvioitiin yksinkertaisella määrällisellä metodilla, jossa riskien vakavuus ja todennäköisyys määriteltiin.

Kehittämistehtävän tulokset osoittavat, että riskejä on tunnistettu huomattava määrä ja niihin on nyt varauduttu paremmin kuin lähtötilanteessa. Täysin kattavaa riskienhallintasuunnitelmaa ei ole pystytty tutkimusajanjaksona luomaan, mutta kaikki vakavat riskit on jo pystytty suunnitelmilla kattamaan. Aikaisemmin tilanteen mukaan toteutetussa riskienhallinnassa on ollut puutteita ja isoon osaan riskeistä ei ollut varauduttu millään keinoin.

Avainsanat	IT-riski, riskienhallinta, riskienhallintasuunnitelma, muutosjohtaminen

Author(s) Title Number of Pages Date	Eric Puchner IT risk management in Company X 48 pages + 6 appendices 2 November 2015
Degree	Master of Business Administration
Degree Programme	Entrepreneurship and Business Competence
Specialisation option	
Instructor(s)	Erkki Sairanen, Senior Lecturer

The aim of this thesis was to study how Company X, a consulting company specialising in recruitment and assessment, can develop its IT risk management and to reveal possible local IT risks. The goal was to create risk management plans for the company. In addition, the study aimed at establishing practices to assess risks and monitor the realized risks.

This was an action research in which risks were assessed with quantitative methods. The applied theory consisted of strategic IT risk management, practical risk management theories and change management theories supporting this research.

Based on the analysis in the beginning of the research, comprehensive risk lists containing locally affecting IT risks were created. Risks were then classified and allocated to groups as decision making is easier when risk planning can be planned by groups instead of by individual risks. Risks were assessed with simple methods by giving every risk a value for severity and probability.

The present research resulted in identifying a considerable number of risks. Additionally, the research inspired the company to prepare for possible risks with risk plans for future reference. The results also point out that the risk management carried out by the company prior to the research has been inadequate and that the company has not been prepared for the majority of the risks found. Risk management plans covering all of the discovered risks were not established during the research period but all serious risks were covered with the plans.

Keywords	IT risk, risk management, risk management plans, change management

Sisällys

1 Johdanto

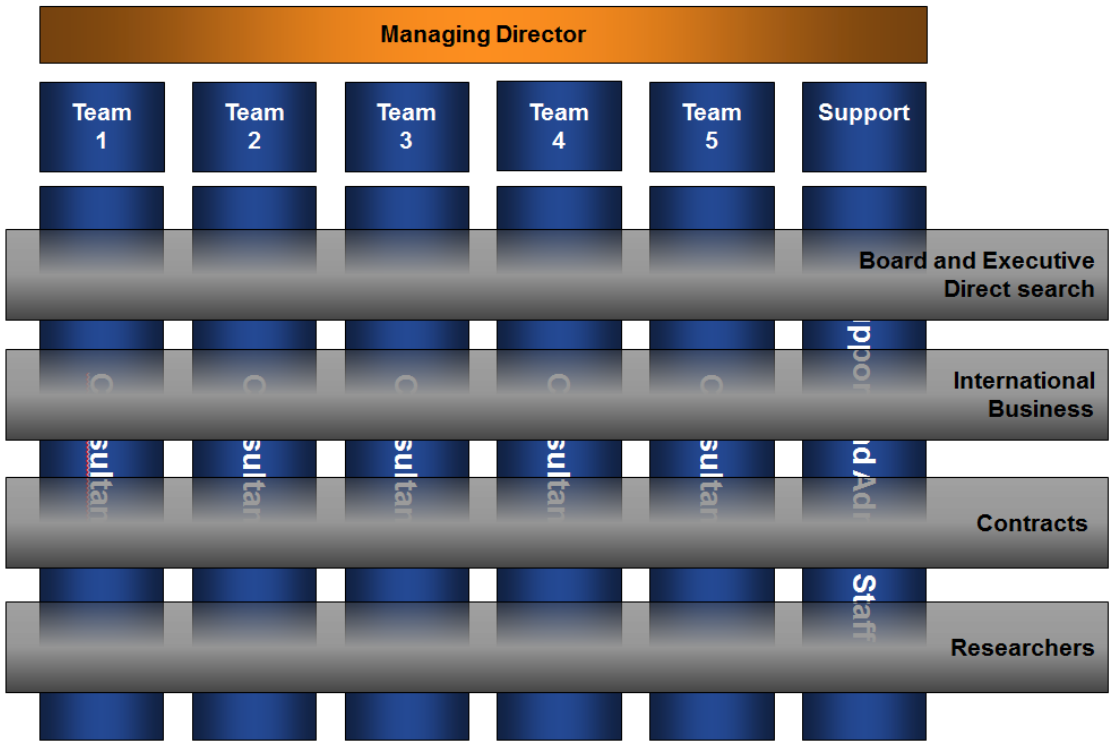
1.1 Yritys

Kehityskohteeksi valittu yritys on keskisuuri konsultointia tarjoava Yritys X. Suomessa yritys toimii koko maan laajuisesti ja sillä on toimipisteet Helsingissä, Turussa, Tampereella ja Oulussa. Kansainvälisesti yritys toimii 24 maassa. Yritys on perustettu vuonna 1967 Ruotsissa. Liikevaihto Suomessa on tällä hetkellä noin 6 miljoonaa euroa vuodessa. Yrityksen päätoimiala on konsultointi ja päätuotteita ovat rekrytointiratkaisut, osaamisen johtaminen, liiketoiminnan muutokset ja ylimmän johdon ratkaisut. Kaikki ratkaisut ovat toteutettavissa ympäri maailmaa asiantuntevien konsulttien toimesta. (Yritys X 2014a.)

Henkilöstöä yrityksellä on Suomessa noin 60. Kansainvälisesti yrityksen palveluksessa on noin 800 konsulttia. Suomessa konsultteja toimii hyvin erilaisilla taustoilla. Yrityksen palveluksessa on muun muassa psykologeja, teologeja, puolustusvoimien palveluksessa olleita ja eri teollisuus- ja teknologia-aloilta konsulteiksi siirtyneitä henkilöitä. Suurin osa konsulteista työskentelee Helsingin toimistolla. Muissa toimipisteissä työskentelee noin 4-8 henkeä per toimisto. Suomessa yritys on toimialansa isoimpia konsultointiyrityksiä ja se on myös tunnetuimpia yritysten johdon keskuudessa. Toiminnan lähtökohta on toiminnan yksinkertaisuus yhdistettynä pitkälle kehitettyihin ratkaisuihin. Asiakkaiden luottamusta pidetään yhtenä tärkeimmistä yrityksen arvoista. Yrityksen visio, strategia ja tavoitteet ovat esitetty erillisessä liitteessä (Ks. liite 1). (Yritys X 2014b.)

Yritys X:llä päätöksenteko on keskitetty muutamalle henkilölle. Lähes kaikki päätökset kulkevat kyseisten henkilöiden kautta ja pienessä organisaatiossa tämä toimii mielestäni hyvin. Kyseinen malli vaikuttaa siihen, että päätökset tulevat nopeasti, koska johto on tottunut päättämään asioita heti ilman kokoontumisia ja neuvotteluja. Yrityksen organisaatio on hyvin matala. Käytännössä koko henkilöstö on yhden tason päässä toimitusjohtajasta ja tämä helpottaa huomattavasti kommunikaatiota yrityksessä kun päätöksiä tarvittaessa ei ole turhia välikäsiä. Lisäksi esimiehet ja johtajat toimivat samoissa tiloissa pääsääntöisesti avoimin ovin, joten kaikki ovat helposti lähestyttävissä ja tavoitettavissa. (Yritys X 2014b.)

Organisaatiokaaviossa, tietohallinto sijoittuu support teamin alle.



Kuvio 1. Organisaatio. (Yritys X 2014b.)

1.2 Tutkimus- ja kehitystehtävän määrittely

Valitsin tutkimuksen aiheeksi yrityksen IT-riskienhallinnan. IT:n tarkoitus on mahdollistaa liiketoiminta ja pyrkimys on, että erilaiset IT:n toimet eivät haittaisi liiketoimintaa. Riskeihin varauduttaessa joudutaan lähes varmasti tilanteeseen, jossa haittoja normaaliin toimintaan tulee ja tasapainoilu hyötyjen ja haittojen välillä tulee olla tietoinen päätös liiketoiminnalta.

Tarkoitukseni on luoda tietohallinnolle selkeät riskienhallinnan käytännöt, joissa toteutuneita tapahtumia arvioidaan, tapahtumia verrataan tiedostettuihin riskeihin ja pyritään reagoimaan riskeihin paremmin. Koska mittareita on melko vähän käytössä tällä hetkellä, on erittäin tärkeää, että työn yhteydessä tutkitaan tarkasti myös jo tällä hetkellä kerätty tieto ja se kuinka pystyisimme hyödyntämään jo olemassa olevaa tietoa mittareita luodessa.

Aihe on yritykselle mielestäni tärkeä. Tällä hetkellä liian paljon jätetään arvion varaan ja osassa riskeistä saatetaan käyttää liikaa resursseja riskin suuruuteen verrattuna, kun taas toisaalla saatetaan säästää hyvinkin korkean riskin torjunnassa ja näin altistaa yrityksen toiminta vaaraan. Yrityksellä olisi hyvä olla selkeä ja yhteen paikkaan koottu ohjeistus, kuinka riskien toteutuessa toimitaan. Tällä hetkellä ohjeita ja käytäntöjä on määritelty useisiin eri paikkoihin ja järjestelmiin.

1.3 Nykytila

Yrityksen pääliiketoimintaan kuuluu rekrytointi. Rekrytointi on muuttunut viime vuosina huomattavasti. Liiketoimintaan on tullut suhteellisen nopealla aikavälillä paljon sähköisiä toimintoja. Ennen hakemukset tulivat pääosin postitse kirjallisina. Projektit saattoivat kestää pitkiä aikoja tämän takia ja hakemusten käsittely, arkistointi ja vanhojen hakemusten hakeminen oli hidasta ja vaati paljon resursseja. Nykyään työpaikkoihin hakeminen on keskittynyt lähes kokonaan Internetiin. Tulevaisuudessa uskon pätevien hakijoiden määrän vähenevän ja kilpailu hyvistä työntekijöistä tulee kovenemaan. Muutokseen pyritään varautumaan kehittämällä toimintaa ja parantamalla järjestelmien toimintaa sekä lisäämällä toiminnallisuuksia, joilla yritys pystyy helposti löytämään potentiaalisia kandidaatteja erilaisiin tehtäviin.

Tulevaisuudessa uskon, että erityisesti teknisesti ala kehittyy vielä. Jo nyt yrityksillä on useita projekteja, joissa video ja interaktiiviset järjestelmät otetaan mukaan rekrytointiin ja alalla tullaan myös entistä enemmän panostamaan rekrytoinnin lisäksi henkilöiden perehdytyksen nopeuttamiseen ja henkilöstön sitouttamiseen. Viimeisten vuosien aikana yrityksessä on tietohallinnon toimesta kehitetty teknistä ympäristöä, käyttäjien osaamista, dokumentaatiota sekä perusasioita, kuten tietoturvaa ja tietosuojaa. Yrityksessä on myös tehty muutoksia rooleihin sekä vastuisiin ja liiketoiminta on ottanut enemmän vastuuta liiketoiminnan järjestelmistä.

Riskeihin ja niiden mahdollisuuteen on yrityksessä varauduttu jollain tasolla, mutta monessa tapauksessa riskejä ei ole tarkasti määritelty ja niiden varalle ei ole tehty selkeitä kirjallisia suunnitelmia. IT-riskit eivät vaikuta yrityksessä suoraan tietohallinnon budjetointiin ja hankintasuunnitelmiin liittyviin päätöksiin. IT-riskejä ja niiden vaikutuksia mitataan yrityksessä vähän. Nykyiseltään käytössä olevat mittarit eivät siis juuri arvioi riskien sekä niiden hallinnan vaikutusta yritykseen.

Käyttäjäkyselyn kautta seurataan henkilöstön toimintaa. Mittarina toimii se, kuinka moni käyttäjistä ilmoittaa toimivansa suosituksien vastaisesti tiedostojen käsittelyssä, tallennuksessa tai tietojen varmuuskopioinnissa. IT-riskejä voidaan tällä hetkellä mitata kriittisten tapahtumien perusteella eli kuinka usein tapahtuu sellaista mitä voidaan pitää yritykselle riskinä. IT-riskejä ja niihin varautumista voitaisiin myös tällä hetkellä arvioida käyttäjien saaman koulutuksen määrällä ja sillä mihin riskeihin koulutuksilla on varauduttu. Lisäksi tietohallinnon kuluja voidaan pitää yhdenlaisena mittarina. Käytössämme on suhteellisen paljon tietoa, jota voidaan käyttää, kun uusia mittareita määritellään.

Iso osa IT-riskienhallinnasta tehtiin aikaisemmin tilanteen mukaan. Hankittaessa uusia laitteita ja ohjelmia, uusia henkilöitä koulutettaessa ja projektien yhteydessä riskejä pyrittiin määrittelemään ja niihin pyrittiin varautumaan mutta selkeää suunnitelmallista IT-riskienhallintaa ei ollut rakennettu.

COBIT:ssa on määritelty kypsyysmalli, jossa prosessin kypsyyttä arvioidaan 0-5 asteikolla. Asteikon tasot ovat kypsyysmallin asteikon mukaiset. Kypsyysmallin asteikot ovat kuvailtuna taulukossa 1.

Taulukko 1. Kypsyysmallin asteikko. (ISACA 2007, 66.)

0 Olematon.	Riskien arviointia, joka vaikuttaisi prosesseihin ja päätöksentekoon, ei ole olemassa. Organisaatio ei arvioi turvallisuusriskien ja kehitysprojektien epäonnistumisten vaikutusta liiketoimintaan.
1 Alustava/tilanteen mukaan	IT-riskejä arvioidaan tilanteen mukaan. Riskit arvioidaan projektikohtaisesti.
2 Toistettava mutta vaistonvarainen	Kehittymätön riskienarviointi on olemassa ja se on otettu käyttöön harkinnanvaraisesti.
3 Määritelty prosessi	Organisaationlaajuinen riskienarviointiprosessi määrittelee milloin ja miten riskienarviointi tehdään. Prosessi on dokumentoitu
4 Hallinnoitu ja mitattavissa	Riskien arviointiin ja hallintaan on standardikäytäntöjä. Yrityksen johdolle raportoidaan kaikista poikkeavuuksista
5 Optimoitu	Riskienhallinta on organisaationlaajuinen, organisoitu ja hyvin hallinnoitu prosessi. Prosessia valvotaan ja tiedon keräys, analysointi ja raportointi ovat hyvin automatisoituja

Tehtävän aloitushetkellä määrittelin yrityksen IT-riskienhallinnan tilaksi 1. Yritys oli varautunut useisiin riskeihin mutta selkeä suunnitelmallinen IT-riskienhallinta oli puutteellinen. Prosessia ei ollut kuvattu selkeästi ja vastuut olivat määrittelemättä suurelta osin. Ongelma ilmeni välillä puutteellisena varautumisena ongelmiin ja siten pidempinä käyttökatkoina verrattuna suunnitelmallisempaan toimintaan.

1.4 Tavoitteet

Ennen opinnäytetyön aloittamista keskustelin esimieheni kanssa mahdollisista aiheista ja tulimme yhdessä siihen tulokseen, että riskienhallinta on hyvä aihe kehittämistehtävälle. Tavoitteeksi asetin selkeän tiedon saamisen päätöksenteon tueksi ja sen, että jatkossa turvataan mahdollisimman paljon yrityksen tietoa ja omaisuutta varautumalla eri riskeihin. Lisäksi asetin tavoitteeksi yrityksen toiminnan suojaamisen ja toiminnan jatkuvuuden takaamisen jatkuvasti muuttuvassa tilanteessa. Tavoitteena oli saada

kaikkiin kriittisiin ja vakaviin riskeihin riskienhallintasuunnitelmat ja mahdollisuuksien mukaan varautua mahdollisimman moniin vähäisempiin riskeihin.

Kehittämistehtävän tuloksena odotin selkeää mallia riskien ryhmittelyyn ja arviointiin sekä riskien toteutumista varten suunnitelmia ja ehkäiseviä toimenpiteitä. Tavoitteena oli myös luoda raportti toteutuneista riskeistä johdolle päätöksentekoa varten. Kypsyysmallin mukaiseksi tavoitetilaksi määriteltiin taso 4.

1.5 Ongelman rajaus

Tutkimuksessa keskitytään Yritys X:n Suomen toimintaan ja siitä on näin ollen rajattu pois sisaryhtiöt sekä emoyhtiön toiminta. Kehittämistehtävä on rajattu koskemaan ainoastaan Suomen organisaatiota ja toimistoja sekä paikallisia järjestelmiä ja laitteita. Aihe rajataan koskemaan ainoastaan IT-riskejä. Muut liiketoiminnan riskit eivät ole tässä työssä tarkastelussa.

1.6 Kehittämistehtävän eteneminen ja aikataulu

Metropolian koulutukseen hakeuduttaessa teimme alustavan suunnitelman opinnäytetyön aiheesta, ja kursseilla jatkettiin suunnittelua kurssitehtävinä. Kehittämistehtävä eteni muiden töiden ohella hitaasti ja välillä tehtävään tuli pitkiäkin taukoja. Alkuperäisen aikataulun mukainen kehittämistehtävän valmistumisaika oli joulukuussa vuonna 2014. En kuitenkaan halunnut kiirehtiä tulosten mittaamisen kanssa ja jätin riittävästi aikaa, jotta sain mitattavia tuloksia myös jatkuvasta seurannasta.

Kehittämistehtävän aikataulu oli seuraava:

- kehittämistehtävän suunnittelu	2012 – 2014
- viitekehys	2013 – helmikuu 2014
- viitekehysseminaari	helmikuu 2014
- alkutilanneselvitys	helmikuu 2014 – kesäkuu 2014
- resurssien arviointi	elokuu 2014 – syyskuu 2014
- riskilistojen laatiminen	syyskuu 2014 – lokakuu 2014
- riskien luokittelu	lokakuu 2014
- jatkuvan seurannan luominen	lokakuu 2014
- riskienhallintasuunnitelmat	marraskuu 2014 –
- toteutuneiden riskien tarkastelu	elokuu 2015
- tulosten analysointi ja raportointi	elokuu – lokakuu 2015
- tulosten esittelyseminaari	lokakuu 2015
- työn valmistuminen	marraskuu 2015

1.7 Tutkimuskysymykset

Tutkimuksen ongelmana on:

- Kuinka yrityksen paikallista IT-riskienhallintaa voidaan kehittää suunnitelmallisemmaksi?

Tutkimusongelmaa selvitettiin tarkemmilla tutkimuskysymyksillä, jotka olivat seuraavanlaisia:

- Kuinka paljon ja kuinka vakavia riskejä havaitaan tekemällä riskikartoitus?
- Kuinka paljon suunnitelmallinen riskienhallinta lisää suunnitelmien ja ohjeistusten määrää yrityksessä?
- Minkälaisia ja kuinka vakavia riskejä, joihin ei yrityksessä ole varauduttu, löydetään siirryttäessä suunnitelmalliseen riskienhallintaan?
- Kuinka paljon riskejä, joita ei ole aikaisemmin havaittu, löytyy jatkuvan seurannan avulla?

1.8 Mittarit

Yrityksen käytössä on kohtalaisesti tietoa, jota voidaan käyttää, kun uusia mittareita määritellään. Koska selkeää suunnitelmaa ei yrityksellä ollut, ei alkutilanteessa voitu myöskään mitata esimerkiksi riskienhallinnan kattavuutta, uusien riskien määrää, niiden toteutuneiden riskien määrää, joita ei ollut prosessissa havaittu ja määritelty sekä esimerkiksi kriittisten IT-riskien määrää. Jatkossa on kuitenkin tarkoitus myös mitata kaikkia edellä mainittuja. Jatkossa voidaan myös mitata sitä, kuinka kulut riskien kartoituksen ja hallinnoinnin myötä muuttuvat ja kuinka suuri osuus kuluista kuluu erilaisiin toimenpiteisiin.

Tämän kehittämistehtävän vaikutuksia mittaan seuraavilla mittareilla:

- Todettujen riskien määrä ja riskiarvot
- Sellaisten kriittisten ja vakavien IT-riskien määrä ja prosenttiosuus, joita varten on tehty riskienhallintasuunnitelma verrattuna suunnittelemattomaan lähtötilanteeseen
- Uusien IT-riskien määrä (ensimmäiseen arvioon verrattuna)
- Niiden merkittävien tapahtumien määrä, jotka aiheutuivat tunnistamattomasta IT-riskistä
- Niiden tapahtumien määrä, joihin löytyy uuden riskienhallintamallin mukainen riskienhallintasuunnitelma
- Riskienhallintasuunnitelmien määrä

Näillä esitetyillä mittareilla pystyin mielestäni vastaamaan tutkimuskysymyksiin ja arvioimaan muutoksen tuloksia. Mittarit määriteltiin siten, että ne mahdollistavat aikataulun mukaisen mittaustulosten saamisen. Pois jätettiin työn aikana muun muassa taloudellisia mittareita, joita ei ollut mahdollista mitata ilman useiden vuosien seurantaa.

2 Kehittämistehtävän viitekehys

Teoreettinen viitekehys kehittämistehtävälle koostuu seuraavista osa-alueista:

1. Strateginen IT-riskien hallinta
2. Riskienhallinnan käytännön toimenpiteet
3. Muutosjohtaminen

IT-riskienhallintaan, määrittelyyn ja varautumiseen löytyy useita erilaisia ja eritasoisia teorioita, joista yritykset voivat valita parhaan omaan tarpeeseensa. Tässä tehtävässä käyn aluksi läpi tunnetuimpia teorioita, ja sen jälkeen keskityn valittuun teoriaan ja käyn teorian vaiheita tarkemmin läpi. IT-riskienhallintaan niissä viitekehyksissä, joita olen tarkastellut, on selkeitä eroja siinä mihin tarkoitukseen ne on luotu. Osa on tarkoitettu IT-johdon käyttöön ja osa taas suorittavan tason ohjaamiseen. Osa on luotu vastaamaan puhtaasti ohjelmistojen kehittämiseen ja toisissa on taas lähtökohtana huomattavasti laajempi kokonaisuus kulunvalvonnasta lähtien johdon päätöksentekoon.

Valitsin alustavaan tarkasteluun tunnetuimpia IT-riskienhallintaa sisältäviä malleja. Ensimmäisenä mallina on Control Objectives for IT and Related Technologies (jatkossa COBIT), joka on IT Governance Instituten luoma viitekehys tietohallinnon johtamiseen. Viitekehyksessä on useita eri aihealueita, joista yksi on Arvioi ja hallinnoi IT-riskejä. Viitekehys on pääsääntöisesti tarkoitettu tietohallinnosta vastaaville ja sen lähtökohtana on luoda yhteys liiketoiminnan ja tietohallinnon välille. Erityisen hyvää viitekehyksessä on sen selkeä ja suhteellisen tiivis kuvaus ohjaukseen tarvittavista tavoitteista ja mittareista. ISACA, joka on julkaissut COBIT:n, on lisäksi julkaissut vuonna 2009 erillisen teoksen The Risk IT Framework, jossa on tarkemmin määritelty riskienhallintaan liittyviä prosesseja.

ISO standardit ovat British Standards Instituten luomia ja ne ovat tuttuja monesta eri aihealueesta. Standardien laajentuessa myös IT-riskien hallintaan on luotu viitekehys ISO 27005. ISO 27005 on luotu toimimaan läheisesti ISO 27000-sarjan standardien kanssa, joissa käsitellään IT turvallisuudenhallintaa yleisemmin.

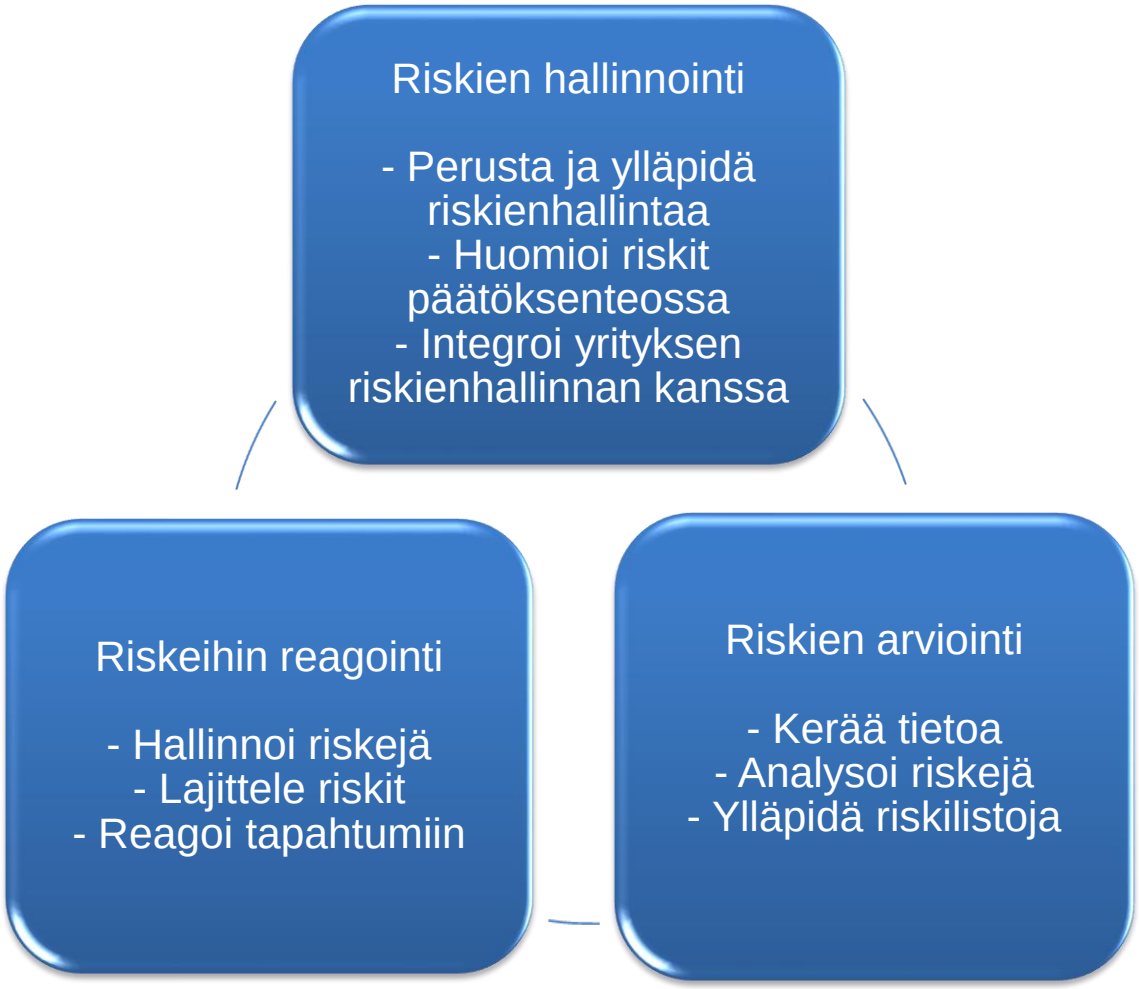
National Institute of Standards and Technology on luonut standardin riskienhallintaan ja se kulkee nimellä SP 800 30 Risk Management Guide for Information Technology Sys-

tems. Standardi on alun perin luotu terveydenhoitoalan ja muiden vastaavien säänneltyjen alojen käyttöön.

Suuri osa kirjallisuudesta, mitä opinnäytetyön aineistoa kerätessäni käsittelin, sisälsi viittauksia COBIT:iin tai ISO 27005 standardiin ja nämä ovatkin kaksi käytetyimpien joukossa olevaa teoreettista viitekehystä IT-riskienhallinnassa. COBIT on selkeä ja siinä on käyty läpi suurin osa IT-riskienhallintaan liittyvistä aihealueista. Olen jo vuosia käyttänyt COBIT:ia, kun olen rakentanut ja kehittänyt yrityksen eri IT-prosesseja. Lisäksi olen käynyt useita COBIT kursseja, joten oli täysin luontevaa jatkaa COBIT:n käyttämistä myös tässä kehittämistehtävässä. ISO standardit ja SP 800 30 vastaavasti eivät ole minulle kovin tuttuja käytännössä ja siksi päätin jättää ne pois tästä opinnäytetyöstä. ISO ja COBIT ovat keskenään hyvin samankaltaisia ja COBIT usein vertaa mitä ISO standardin kohtaa kyseinen prosessi vastaa.

2.1 Riskienhallinnan malli

The Risk IT Frameworkissa prosessi on jaettu kolmeen päätasoon, joiden alla on kolme alempaa tasoa, joilla jokaisella on omia toimenpiteitä.



Kuvio 2. IT-riskienhallinnan prosessit. (ISACA 2009, 15)

COBIT:ssa löytyy prosessi APO12 Hallinnoi riskejä. Prosessi määritellään kirjassa seuraavanlaisesti: Jatkuvasti tunnista, arvioi ja vähennä IT-sidonnaisia riskejä johdon määrittelemissä rajoissa (ISACA 2012, 107.).

Prosessissa on määritelty korkeamman tason tavoitteet ja toimenpiteet riskienhallinnalle, mutta siinä ei ole käytännön toimenpiteitä tai sitä kuinka toimenpiteitä tulisi toteuttaa.

2.2 Riskien arviointi

Käsittelen seuraavaksi COBIT:n määrittelemiä prosessin osia ja niille määriteltyjä toimenpiteitä niiltä osin, kuin näen käytännölliseksi suorittaa yrityksessämme. Riskien arvioinnilla pyritään saamaan jokaiselle riskille arvo, jolla niiden vakavuutta voidaan arvioida. Arviointi on jaettu osiin, jotka ovat tiedonkeruu, riskien analysointi sekä riskilistojen luominen.

2.2.1 Tiedonkeruu

COBIT:ssa on määritelty useita toimenpiteitä oleellisen tiedon keräämiseen ja tehokkaan IT-riskien tunnistamisen luomiseen, analysoinnin ja raportoinnin mahdollistamiseksi. Yrityksen tulisi luoda ja ylläpitää mallia IT-riskien tunnistamiseen, ryhmittelyyn ja analysoimiseen. Mallissa olisi hyvä olla useita tapahtumatyyppejä, luokitteluja sekä riskikertoimia. Relevanttia tietoa tulisi kerätä yrityksen sisäisestä ja ulkoisesta toimintaympäristöstä, joilla voi olla vaikutus IT-riskienhallintaan. Tiedon keruussa oleellisena osana tulisi tutkia ja analysoida historiatietoa IT-riskeistä ja tiedon häviöistä ulkoisista tietolähteistä, trendeistä ja tietokannoista. (ISACA 2012, 109.)

COBIT:n mukaan tiedot tulisi kirjata kaikista riskeistä, jotka ovat aiheuttaneet tai mahdollisesti aiheuttavat vaikutuksia IT-projekteihin, IT-toimintoihin ja palveluntuottamiseen. Oleellista tietoa olisi hyvä kerätä myös ongelmista, tapahtumista ja selvityksistä. Riskit tulisi luokitella samanlaisiin ryhmiin ja yhteneväisiä tekijöitä tulisi korostaa. Riskien toteutumiseen johtaneiden tapahtumien yhteisiä tekijöitä olisi hyvä määritellä. Olisi hyvä seurata erityisiä edellytyksiä, joita ilmeni tai oli poissa, kun riski toteutui. Samalla tulisi seurata kuinka tapahtumien aikaiset olosuhteet toimintaympäristössä vaikuttivat tapahtumien toistumiseen ja tappioiden määrään. Säännöllisillä tapahtuma- ja riskikerroinanalyyseillä pyritään tunnistamaan uusia tai nousevia riskejä sekä saadaan ymmärrystä ulkoisista ja sisäisistä riskeihin vaikuttavista tekijöistä. (ISACA 2012, 109.)

2.2.2 Riskien analysointi

Riskien analysointi toteutetaan luomalla hyödyllistä tietoa, joka ottaa huomioon liiketoiminnan kannalta oleelliset riskitekijät riskienhallinnan päätösten tueksi. Toimenpitei-

nä tulisi määritellä sopiva tarkkuus riskien analysointiin, jossa huomioidaan kaikki riskiluokat ja resurssien liiketoimintakriittisyys. (ISACA 2012, 109.)

IT-riskisuunnitelmia tulisi rakentaa ja päivittää jatkuvasti. Riskisuunnitelmien tulisi pitää sisällään kaikki uhkatyypit. IT-riskien mahdollisten tappioiden tai voittojen todennäköisyys ja laajuus tulisi arvioida riskien analysoinnin yhteydessä. Yrityksen tulisi tunnistaa haavoittuvuudet, jotka vaativat riskienhallintaa ja analysoida potentiaaliset riskientorjuntavaihtoehdot, kuten riskin välttäminen, riskin vähentäminen, riskin siirtäminen ja riskin hyväksyminen. Riskisuunnitelmissa tulisi ehdottaa optimaalista riskeihin reagointia. (ISACA 2012, 109.)

Bill Holstnider ja Brian D. Jaffe määrittelevät, että riskejä voidaan analysoida kahdella tavalla.

- Määrällinen metodi, jossa riskeille annetaan lukuarvoja esimerkiksi riskin vaikutuksista yrityksen toimintaan, tai kustannukseen, jolla riskiltä suojaudutaan. Lisäksi arvioidaan kuinka usein riski saattaa toteutua.
- Laadullinen metodi, jossa riskiä arvioidaan kokemusten, näkemyksen ja käsitysten perusteella. Arviosta pyritään tekemään mahdollisimman puolueeton.

(Holstnider & Jaffe 2010, 229.)

Shon Harris on vertaillut määrällisen ja laadullisen metodin eroja mielestäni hyvin ja yksinkertaisesti taulukossa 2.

Taulukko 2. Määrällisen ja laadullisen metodin erot. (Harris 2008, 101)

Ominaisuus	Määrällinen	Laadullinen
Ei vaadi laskentaa		X
Vaatii vaativaa laskentaa	X	
Pitää sisällään paljon arvailua		X
Tuottaa yleisiä riskialueita ja viittauksia riskeihin		X
On helpompi automatisoida ja arvioida	X	
Käytetään riskienarvioinnin toimivuuden seurantaan	X	
Tuottaa luotettavan hinta/hyöty analyysin	X	
Käyttää erikseen päteviä ja objektiivisia arvoja	X	
Käyttää niiden tahojen mielipiteitä, jotka tuntevat prosessin parhaiten		X
Näyttää selkeitä tappioita, joita voi koitua vuoden sisällä	X	

Harrisin mukaan riskien analyysiä varten tulisi määritellä arvot jokaiselle voimavaralle vastaamalla seuraaviin kysymyksiin:

- Mikä on voimavaran arvo yritykselle?
- Kuinka paljon sen ylläpito maksaa?
- Kuinka paljon se tekee voittoa yritykselle?
- Kuinka paljon sen arvo olisi kilpailijalle?
- Kuinka paljon sen uudelleen hankinta tai korjaaminen maksaisi?
- Kuinka paljon sen hankinta tai kehittäminen maksoi?

(Harris 2008, 94.)

Seuraavaksi Harrisin mukaan tulisi arvioida mahdolliset menetykset riskiin liittyen vastaamalla seuraaviin kysymyksiin:

- Mitä fyysistä vahinkoa voisi riskin toteutuminen aiheuttaa ja kuinka paljon se maksaisi yritykselle?
- Kuinka paljon riskin toteutuminen voisi haitata tuottavuutta ja kuinka paljon se maksaisi yritykselle?
- Kuinka paljon menetetään jos luottamuksellista tietoa katoaa?
- Kuinka paljon maksaa selviytyä riskin toteutumisesta?
- Kuinka paljon maksaisi, jos kriittiset laitteet hajoaisivat?
- Mikä on yksittäinen menetyksen arvio jokaiselle voimavaralle ja jokaiselle riskille?

(Harris 2008, 94.)

Riskianalyysin kolmas vaihe Harrisin mukaan tulisi olla jokaisen riskin arviointi. Pitäisi arvioida mikä on todennäköisyys riskien toteutumiselle sekä laskea jokaiselle riskille vuosittainen toteutumistiheys, joka ilmaisee kuinka monta kertaa riski voi toteutua vuoden aikana. Tämän jälkeen viimeisenä vaiheena tulisi yhdistää mahdolliset riskien arvot ja todennäköisyydet ja hyödyntää näitä arvoja riskienhallinnassa sekä verrata riskeiltä suojautumisen hyöty-/kustannussuhteita riskien toteutumisen aiheuttamiin kuluihin. (Harris 2008, 95.)

2.2.3 Riskilistojen luominen

COBIT:n mukaan riskilistat tulisi muodostaa luomalla ja ylläpitämällä luetteloa tunnetuista riskeistä ja riskien ominaisuuksista, kuten riskin yleisyys, mahdollinen vaikutus ja toimenpiteen. Lisäksi listassa tulisi olla resurssit, jotka riskiin liittyvät sekä olemassa olevat toimenpiteet. Riskilistojen luomisen yhteydessä liiketoimintaprosessit tulisi inventoida. Inventoinnin tulisi pitää sisällään henkilöstön, sovellukset, infrastruktuurin, tilat, kriittiset manuaaliset tiedot, toimittajat, yhteistyökumppanit ja ulkoistetut palvelut. Liiketoiminnan jatkuvuuden kannalta oleelliset IT-palvelut ja resurssit tulisi määritellä ja hyväksyttää johdolla. Yrityksen tulisi kerätä säännöllisesti kaikki riskiarviot ja liittää ne koottuihin riskilistoihin. Riskiarvioiden perusteella tulisi määrittää riskisuunnitelmiin riskien aiheuttajia, jotta riskien toteutuminen voidaan tunnistaa nopeasti. (ISACA 2012, 110.)

Eerola ja Luoto ovat ryhmitelleet riskit eri perusteilla tarkastelutilanteen asettamien tarpeiden mukaan. Ryhmittelyn perusteena voi olla esimerkiksi:

- riskin muodostuminen yrityksessä tai sen ulkopuolella
- riskinotto: tietoinen/tiedostamaton
- riskin ilmeneminen: välitön/välillinen
- riskin kohde: pääomariski, tuoteriski, markkinariski jne.
- seurausten vakavuus
- toteutumisen todennäköisyys

(Eerola & Luoto 2000, 24.)

Vastaavasti Jordan ja Silcock ovat ryhmitelleet IT-riskit seuraavalla luokittelulla:

- Projektit, jotka eivät valmistu – ainakaan sellaisina kuin piti
- IT-palveluiden jatkuvuus – kun liiketoiminta lamaantuu
- Tieto-omaisuus, joka ei pysy tallessa
- Palveluntarjoajat ja IT-toimittajat: katkoksia tietotekniikan arvoketjussa
- Sovellukset: murenevat järjestelmät
- Infrastruktuuri: hyllyvä perusta
- Strategiset riskit ja tulevaisuuden uhat: kun IT tekee kyvyttömäksi

(Jordan & Silcock 2006, 60.)

2.3 Riskeihin reagointi

Riskeihin tulisi reagoida viestimällä riskeistä. Tarkoituksena on tuottaa tietoa oikea-aikaisesti IT-riskien nykytilasta ja mahdollisuuksista, kaikille sidosryhmille, jotta ne voivat tehdä sopivia vastatoimia. (ISACA 2012, 110.)

Riskeistä tulisi raportoida kaikille sidosryhmille järkevässä ja selkeässä muodossa päätöksentekoa varten. Riskienhallinnassa tulisi tuottaa päätöksentekijöille tietoa pahimmista mahdollisista tilanteista ja todennäköisimmistä tilanteista. Lisäksi tulisi tuoda esille sellaiset riskit, joissa on mukana maineeseen vaikuttavia sekä lakien ja säädösten noudattamiseen vaikuttavia tekijöitä. (ISACA 2012, 110.)

Kaikille sidosryhmille tulisi raportoida nykyinen riskiprofiili ja jos mahdollista kolmannen osapuolen tulisi tarkastella raportteja sekä sisäisiä tarkastuksia. Näiden tuottama tieto tulisi liittää riskiprofiileihin. (ISACA 2012, 110.)

2.3.1 Riskienhallintakeinot

Riskien välttäminen tarkoittaa sitä, että vältetään toimenpiteitä, jotka mahdollistavat riskien toteutumisen. Yleensä riskien välttämistä käytetään silloin, kuin mikään muu riskienhallinnan keino ei toimi ja kun jokin seuraavista todetaan:

- Ei ole muita kustannustehokkaita keinoja riskin suuruuden tai esiintymistiheyden vähentämiseksi
- Riskiä ei voida siirtää tai jakaa
- Johto ei hyväksy riskiä

(ISACA 2012, 28.)

Riskien vähentämisellä pyritään havaitsemaan riskejä, jonka jälkeen tehdään toimenpiteitä, joilla vähennetään riskin suuruutta tai esiintymistiheyttä. Riskejä voidaan myös jakaa tai siirtää. Osa riskistä voidaan siirtää esimerkiksi ulkoistamalla tai vakuuttamalla. Voidaan esimerkiksi ottaa vakuutus IT-laitteistoille, ulkoistaa osa toiminnasta tai jakaa riski toimittajille tekemällä sopimuksia, joissa määritellään kiinteät hinnat tai jaetaan investoinnin kulut. Nämä keinot eivät kuitenkin vapauta yritystä riskeistä mutta ne saattavat tuoda yritykselle osaamista riskinhallintaan yhteistyökumppanilta tai jakaa taloudellisia seurauksia riskien toteutuessa. (ISACA 2012, 28.)

Riskejä voidaan myös hyväksyä, jolloin niiden varalle ei tehdä mitään toimenpiteitä ja tappiot hyväksytään, jos riski toteutuu. Tämä ei kuitenkaan tarkoita, että riskien suhteen ollaan välinpitämättömiä. Riskin hyväksyminen tarkoittaa, että riski on tunnistettu ja on tehty tietoinen päätös johdon toimesta hyväksyä riski sellaisenaan. Erityisesti IT-riskit tulisi hyväksyä ainoastaan johdon toimesta IT:n tukemana ja riskien hyväksyminen tulisi viestiä johdolle sekä hallitukselle. (ISACA 2012, 28.)

2.3.2 Riskienhallinnan toimenpidesuunnitelma

Riskienhallintaa varten tulisi tehdä toimenpidesuunnitelmia. Toimenpidesuunnitelmien avulla riskejä pyritään pienentämään hyväksytylle tasolle. Toimenpidelistassa tulisi olla määriteltynä kyseiseen riskiin liittyvät resurssit, vastuuhenkilöt sekä toimenpidesuunnitelmat. (ISACA 2012, 111.)

Toimenpidesuunnitelmissa tulisi myös olla listattuna, kuinka organisaatio seuraa riskejä ja niiden mahdollisia aiheuttajia. Lisäksi yrityksen tulisi luoda lista projekteista ja toimenpiteistä, jotka on suunniteltu riskien vähentämiseen. (ISACA 2012, 111.)

2.3.3 Tapahtumiin reagointi

COBIT:ssa todetaan, että riskeihin tulisi reagoida oikea-aikaisesti tehokkailla keinoilla, jotta voidaan rajoittaa IT-riskien aiheuttamien menetysten laajuutta. Tämä voidaan tehdä valmistelemalla, ylläpitämällä ja testaamalla suunnitelmia, joissa on dokumentoitu toimenpiteet, joita tulee tehdä, kun riskin toteutuminen havaitaan. (ISACA 2012, 111.)

Tapahtumia tulisi luokitella ja niitä tulisi verrata määriteltyihin rajoihin. Tapahtumien vaikutukset liiketoimintaan tulisi kommunikoida raportoinnin yhteydessä ja riskilistat sekä riskisuunnitelmat tulisi päivittää. Riskien toteutuessa yrityksen tulisi vaikutuksien minimoimiseksi toteuttaa suunniteltuja toimenpiteitä. (ISACA 2012, 111.)

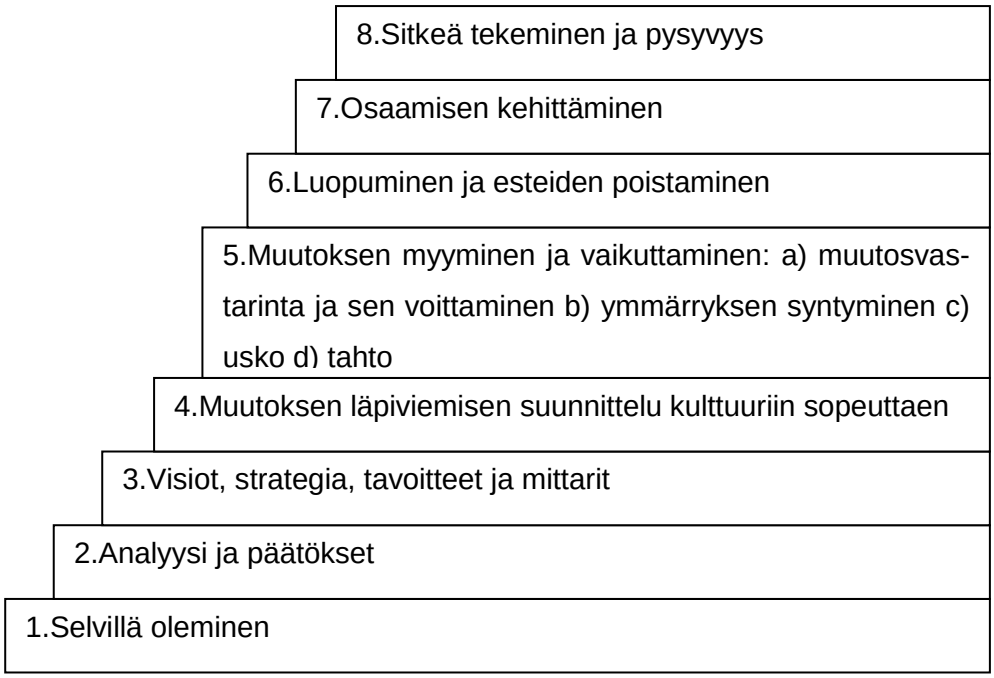
2.4 Muutosjohtaminen

Erolan ja Luodon mielestä systemaattisen riskienhallinnan esteinä on yrityksissä monia tekijöitä. Uuden prosessin mukanaan tuoma lisätyö koetaan rasitteeksi tai riskienhallin-

taa pidetään vain yhtenä uutena järjestelmänä, jonka puitteissa pyöritetään byrokratiaa ja täytetään uusia lomakkeita. Organisaatiolla ei ole useinkaan olemassa varautumissuunnitelmia poikkeustilanteiden varalle. Suunnitelmiin ei myöskään nähdä tarvetta, koska ennenkin on pärjätty ilman. (Erola & Luoto 2000, 61.)

Erola ym. Mukaan tyypillinen este suunnitelmien tekemiseen on se, että siihen ei ole aikaa. Yrityksen johdon arvoista ja painotuksesta riippuu, mitkä tehtävät ovat niin tärkeitä, että aika niihin riittää. Mikäli riskien kartoitusta ja varamenettelyjen suunnittelua ei pidetä johdon mielestä tärkeänä asiana, ei niihin myöskään voida organisaatiossa panostaa ja käyttää aikaa. (Erola ym. 2000, 61.)

Erilaisten esteiden välttämiseksi, ja koska kehittämistehtävässä haetaan muutosta yrityksen toimintaan, on muutosjohtamista hyvä käsitellä kevyesti. Erämetsä (2004, 154) on luonut kuvion 3 mukaisen Läpiviemisen portaat, joka on muunnelma Kotterin Muutoksen portaat -mallista. Läpiviemisen portaat -mallin pääpaino on muutoksen läpiviemisen suunnittelussa, muutoksen myymisessä ja konkreettisessa ihmistyössä, ja mielestäni se soveltuu hyvin tilanteeseemme.



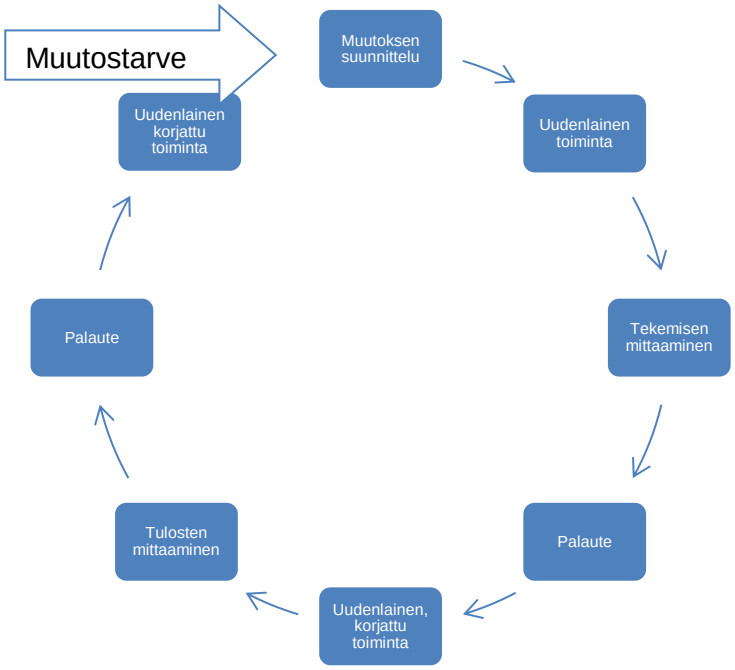
Kuvio 3. Läpiviemisen portaat. (Erämetsä 2004, 154)

Erämetsän mielestä olisi ihanteellista, jos muutoksessa asenteiden muokkaaminen ja hienosäätäminen tulisi ennen konkreettista muutosta. Parhaimmillaan asenteita yhdessä muuttamalla ja kehittämällä voidaan saada ihmiset oivaltamaan muutoksen tarve ja mahdollisesti paremmat ratkaisut, kuin mitä olisi saatu suoraan läpiviemisellä. (Erämetsä 2004, 108.)

Erämetsä toteaa, että silloin kun on kriittisen tärkeää viedä muutos läpi nopeasti, on pakko noudattaa perinteistä tapaa: aloittaa vaatimalla toimintatavan muutosta. Tällöin vaatimisen tulee olla nimensä veroista, eikä vaihtoehtoja voi eikä saa antaa. Järjestelmän, työkalun tai menetelmän käyttämisestä tulee pakko. Pakon ja ulkoapäin ohjautumisen tunteita voidaan lieventää jatkuvalla kommunikaatiolla muutoksen yhteydessä. (Erämetsä 2004, 109.)

Muutoksien ongelmana on aika. Kulttuurin todellinen muuttaminen on vaikeaa ja kestää tavallisesti vuosia. Asenteisiin, ajatteluun, uskomuksiin, arvoihin ja normeihin vaikuttaminen tulisi alkaa viimeistään muutoksen alkuvaiheessa. (Erämetsä 2004, 110.)

Muutoksen mittaaminen on oleellinen osa opinnäytetyötä ja muutoksia tulisi mitata ja arvioida säännöllisesti. Erämetsän (2004, 175-176) mukaan mittaamatta jättäminen on varma keino tehdä muutoksesta epäselvä ja hahmoton. Kuitenkin on vaarana vajota ylimittaamiseen ja etenkin merkityksettömien asioiden mittaamiseen. Mittaamisen ja seurannan onnistumisen edellytykset luodaan yksinkertaisuudella. Erityisesti muutoksen silmässä on syytä huolehtia siitä, että mitataan vain oikeita asioita. Kuviossa 4 on kuvattu mittareita muutoksen pyörässä.



Kuvio 4. Mittareita muutoksen pyörässä. (Erämetsän 2004, 175-176)

Arikoski ja Sallinen kuvaavat muutoksen johtamisen työkaluja, joista olen poiminut tähän tehtävään mielestäni sopivia. Tiedottamisen tärkeyttä muutoksen johtamisessa ei voi korostaa. Jos muutosta on valmisteltu kovin kauan antamatta siitä tietoa työntekijöille, voi muutoksen julkistamisen yhteydessä syntyä konflikti johdon ja henkilöstön välille. Ideaalisin tapa tiedottaa muutoksesta on sellainen, joka saattaa johdon ja henkilöstön tunnereaktiot mahdollisimman lähelle toisiaan. Tämä on mahdollista runsaalla tiedonvälityksellä, kysymykset sallivalla vuorovaikutuksella ja henkilöstön ottamisella mukaan suunnitteluun ja toteutukseen. (Arikoski & Sallinen 2007, 91-92.)

Opi tuntemaan ihmiset ja anna heidän tutustua itseesi on seuraava muutoksen johtamisen keino, jota käytän. Joskus organisaatiossa on ryhmiä, jotka ovat toimineet muuttumattomissa olosuhteissa pitkiä aikoja. Tällaisessa ryhmässä pienikin muutos saattaa aiheuttaa tunteenpurkauksia ja yllättävän rajua muutosvastarintaa. Ihmisiin tutustuminen ei voi olla yksisuuntaista toimintaa. Ei riitä, että opettelee tuntemaan työntekijät, jos ei anna muiden tutustua vastavuoroisesti itseensä. Ihmisten tunteminen onnistuu vain menemällä heidän luokseen. Tiukoissa kriisitilanteissa pelkkä näyttäytyminen saattaa rauhoittaa ihmisiä. (Arikoski ym. 2007, 96.)

Arikosken ja Sallisen mielestä eräs parhaita tapoja sitouttaa henkilöstö eli saada ihmiset omistautumaan muutokselle on ottaa työntekijät mukaan muutoksen suunnitteluun tai ainakin sen toteutukseen. Tätä keinoa usein väheksytään ja aliarvioidaan. Sitouttamisen edellytyksenä on, että jokaiselle löytyy sopiva ja mielekäs rooli. (Arikoski ym. 2007, 99)

Hankalimpia tilanteita sitouttaa ihmisiä muutokseen Arikosken ja Sallisen mukaan ovat tilanteet, joissa muutoksen vetäjä ei ole itse vielä omistautunut muutokselle tai jota hän ei vielä edes hyväksy. Tällöin ei ole juuri vaihtoehtoja. Muutoksen vetäjän tulee ensin itse sitoutua muutokseen, jotta hän voi johtaa muutosta omalla esimerkillään. Esimerkillä johtaminen ei tarkoita muiden töiden tekemistä vaan omien työtehtävien suorittamista muuttuneiden olosuhteiden ehdoilla siten, että muut havaitsevat muuttuneen toiminnan. (Arikoski ym. 2007, 100.)

Valmennus ja koulutuksen järjestäminen ovat oleellinen osa muutoksien johtamista. Arikoski ja Sallinen toteavat, että valmennukset ovat oppimistilaisuuksia, joissa asiantuntija pyrkii tarjoamaan neuvoja, vinkkejä ja esimerkkejä sekä samalla hyödyntämään osallistujien ammattitaitoa tulevien haasteiden voittamiseksi. Parasta valmennuksessa on henkilöstön omien voimavarojen, osaamisen ja kokemusten valjastaminen muutoksen hyväksi. Valmennus on tuottanut tulosta vasta, kun organisaation ihmiset toimivat muutosta edistävällä tavalla. (Arikoski ym. 2007, 111.)

3 Tutkimusmenetelmä

Opinnäytetyö toteutettiin toimintatutkimuksena. Heikkinen, Rovio ja Syrjälä toteavat kirjassaan Toiminnasta tietoon, että toimintatutkimuksessa tuotetaan tietoa käytännön kehittämiseksi. Siinä tutkitaan ihmisten toimintaa. Toimintatutkimuksessa kehitetään käytäntöjä entistä paremmiksi järkeä käyttämällä. Toimintatutkimus kohdistuu erityisesti sosiaaliseen toimintaan, joka pohjautuu vuorovaikutukseen. (Heikkinen & Rovio & Syrjälä 2007. 16-17.)

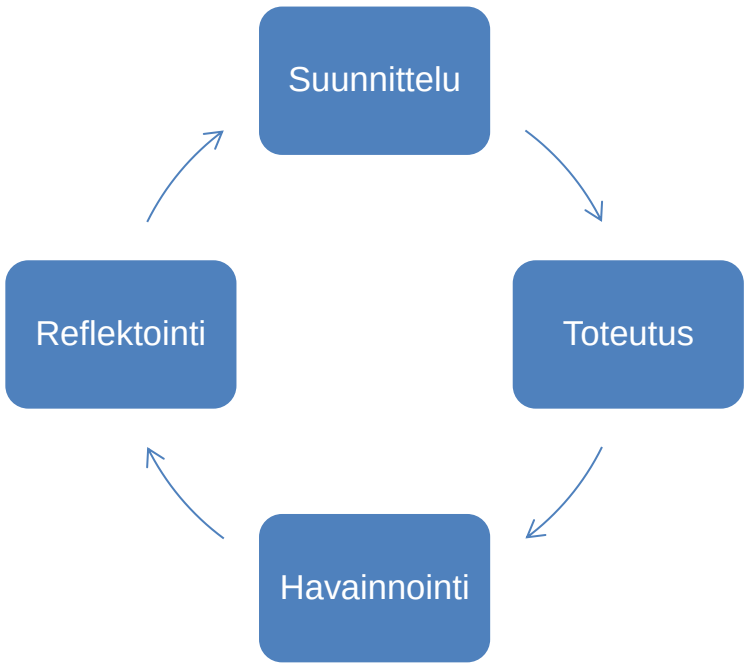
3.1 Toimintatutkimus

Toimintatutkimus on yleensä ajallisesti rajattu tutkimus- ja kehittämisprojekti, jossa suunnitellaan ja kokeillaan uusia toimintatapoja. Toiminnan laajuuden mukaan toimintatutkimus voidaan jakaa viiteen analyysitasoon:

1. yksilö
2. ryhmä
3. ryhmien väliset suhteet
4. organisaatio
5. alueellinen verkosto, kuten yritysten, kuntien, koulutuksen ja tutkimuksen yhteinen strategia

(Heikkinen ym. 2007. 17-18.)

Heikkinen ym. toteavat, että toimintatutkimus on prosessi, jossa ymmärrys ja tulkinta lisääntyvät vähittäin. Kun tutkimuksessa perinteisesti kiinnitetään huomiota siihen, miten asiat ovat, toimintatutkimuksessa ajatellaan, miten asiat ovat olleet ja mihin suuntaan ne ovat menossa. Heikkinen ym. kuvaavat toimintatutkimuksen sykliä kuviossa 5. (Heikkinen ym. 2007, 36.)



Kuvio 5. Toimintatutkimuksen sykli. (Heikkinen ym. 2007. 17-18)

Toimintatutkimus luokitellaan usein tutkimusoppaissa laadulliseksi tutkimusmenetelmäksi. Käsitys on yleinen mutta Heikkinen ym. mielestä osin virheellinen. Toimintatutkimuksessa voidaan käyttää myös määrällisiä tiedonhankintamenetelmiä. Lisäksi toimintatutkimus ei ole varsinaisesti tutkimusmenetelmä vaan lähestymistapa tai asenne, jossa tutkimus kytketään toiminnan kehittämiseen. (Heikkinen ym. 2007, 36-37.)

3.2 Aineistonhankintamenetelmät

Aineiston hankinnassa käytettiin alan julkaisuja ja kirjallisuutta sekä havainnointia. Oma tietämykseni alasta ja yrityksestä toimi pohjana työssä, ja tutkimuksen aikana opituilla tiedoilla vahvistettiin IT-riskien tuntemusta ja osaamista riskeihin varautumisen keinoista. Pyrin käyttämään mahdollisimman uutta tietoa, koska IT alana on kehittynyt viimeisten vuosien aikana nopeasti ja tieto vanhentuu suhteellisen nopeasti.

Keräsin yritykseen liittyvää tietoa yrityksen verkkosivuilta, Intranetistä, vanhoista tiedotteista ja ilmoituksista. Lisäksi käytössä oli henkilöstökäsikirja, tietohallinnon ohjeistukset sekä perehdytysmateriaalit. Yritystä ja sen toimintaa sekä liiketoimintaympäristön muutoksia arvioin omalta työskentelyajaltani, joka alkoi vuoden 2011 keväällä.

Käytin riskilistan keräämiseen alan kirjallisuutta ja julkaisuja sekä Internet-lähteitä. Löysin Internetistä hyvin kattavan Saksan tietoturvaviraston IT-Grundschutz-Catalogues, joka piti sisällään kaikki työssä käytetyt riskit joko suoraan tai muokattuna yrityksellemme soveltuviksi. Muut kirjallisuudesta löytyneet IT-riskilistat olivat yleensä joko hyvin yleisellä tasolla, vanhentuneita tai suppeita.

Palvelupyynnöistä palveluntarjoajalle ja toimenpidepyynnöistä kansainväliselle organisaatiolle kerättiin toteutuneita riskejä vuoden 2012 alusta eteenpäin aina vuoden 2015 elokuulle. Palveluntarjoajan palvelupyynnöt saimme suoraan järjestelmästä mutta toimenpidepyynnöistä kansainväliselle organisaatiolle piti käydä läpi huomattava määrä sähköposteja. Osaa toimenpidepyynnöistä ei saatu selville, koska vuoden 2013 aikana siirryimme käyttämään support tool -työkalua, josta ilmoitukset menevät suoraan asiaa hoitavan pääkäyttäjän sähköpostiin eikä siten niistä ei jää tietoa lähettäjälle tai järjestelmiin.

Kokosin aineiston pääasiassa Microsoftin Excel-tiedostoon, jossa tiedon muokkaaminen, erilaiset laskennat ja tietojen siirtäminen oikeisiin ryhmiin on helppoa. Lisäksi käytin Microsoftin Word-ohjelmaa riskienhallintalomakkeen tekemiseen.

Suoritin tietohallinnon kyselyn yrityksen henkilöstölle vuoden 2014 toukokuussa. Kehittämistehtävään liittyvä kysymys lisättiin tietohallinnon vuosittaiseen kyselyyn ja kysely suoritettiin Surveypal -kyselytyökalulla. Kyselyyn vastasi yhteensä kolmekymmentäviisi työntekijää viidestäkymmenestäkuudesta. Riskejä koskevaan kysymykseen tuli yhteensä kymmenen yksittäistä vastausta yhdeksältä käyttäjältä eli vastausprosentiksi kysymykseen jäi kuusitoista prosenttia.

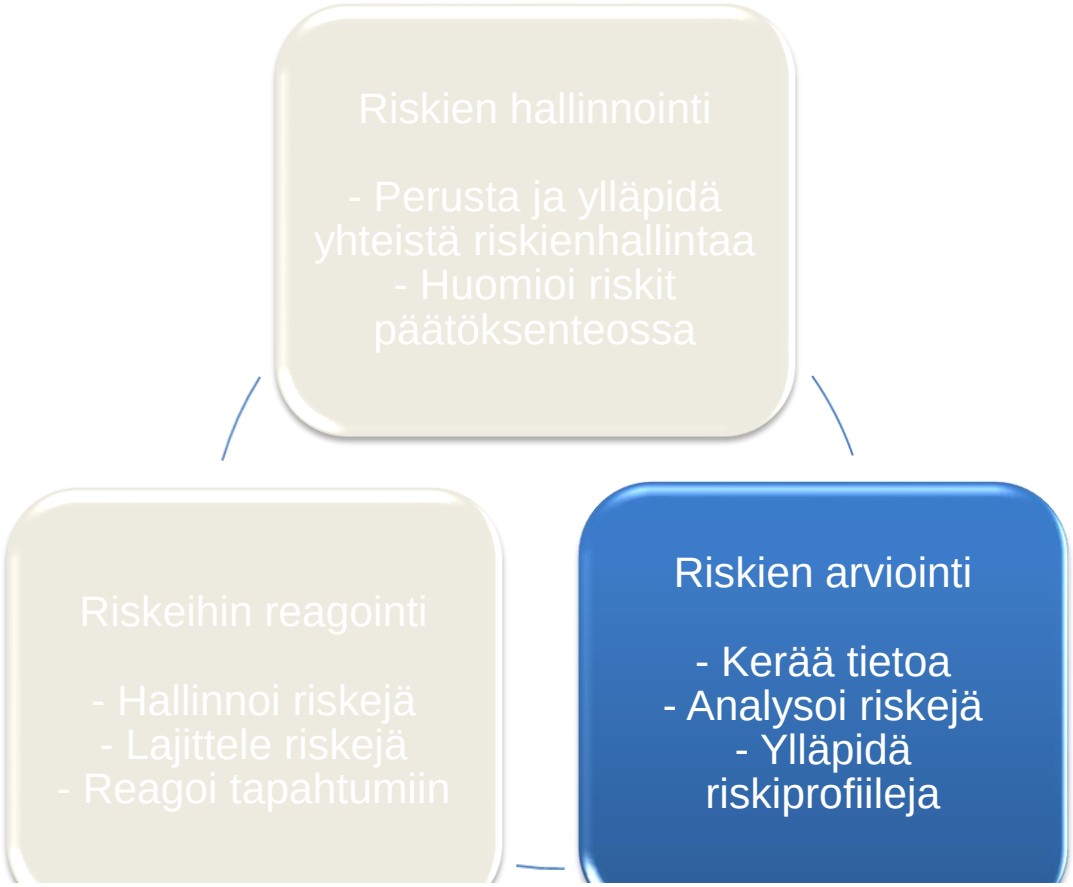
Tutkimuksen varhaisessa vaiheessa rajasin alkuperäisestä suunnitelmasta pois käyttäjiin liittyvät vaikutukset. En nähnyt siksi järkeväksi uusia kyselyä tämän työn puitteissa ja suunnitellut haastattelut ja kyselyillä tehtävät selvitykset riskienhallinnan vaikutuksista käyttäjien toimintaan jäivät pois.

4 IT-riskienhallinnan toteutus

Tässä kappaleessa kuvataan, kuinka riskienhallinnan kehittämistehtävä eteni käytännössä ja minkälaisia vaiheita kehittämistehtävässä oli. Kappaleessa käydään läpi riskien arvioinnin ja riskeihin reagoinnin toteutus.

4.1 Riskien arvioinnin toteutus

Kuviossa 6 korostettuna COBIT:ssa määritelty riskien arviointiprosessi ja sen osat.



Kuvio 6. Riskien arviointiprosessi. (ISACA 2009, 15)

Aloittaessani kehittämistehtävän tekemisen keräsin COBIT:n teorian mukaisesti ensimmäiseksi kaikki mahdolliset IT-ohjeet, joita yrityksellä on, sekä paikallisesti, että kansainvälisesti. Näissä ohjeissa oli suurin osa käyttäjille annetuista ohjeista siitä kuinka ongelmatilanteissa toimitaan. Lisäksi keräsin kaikki koulutus- ja perehdytysmateriaalit. Aineiston keruu oli vaivatonta, koska olen itse kirjoittanut suuren osan tällä hetkellä käytössä olevista materiaaleista.

Osa riskeistä liittyy yrityksen yhteistyökumppaneihin ja tavaran- sekä palveluntoimittajiin, joten kävin läpi kaikki oleelliset sopimukset ja mahdolliset riskien aiheuttajat, sekä minkälaisia riskeiltä suojautumiskeinoja sopimuksissa oli.

Aikaisemmat toteutuneet riskit kirjasin muistista suoraan riskilistaan. Hain tiedot riskilistausta varten käytössämme olevasta järjestelmästä, jolla ilmoitetaan kansainväliselle organisaatiolle tapahtuneista ongelmista, esimerkiksi palomuurien kanssa, sekä järjestelmästä, jolla ilmoitetaan Citrix -palveluntarjoajalle virtuaaliympäristöön kohdistuneista ongelmista. Haastavinta tässä vaiheessa oli muistaa erilaisia tapahtumia ja niihin johtaneita syitä. Lista oli hyvin tekniikkapainotteinen, koska niistä jäi järjestelmiin useammin merkintä tai tilaus esimerkiksi tavarantoimittajalle. Erillisessä liitteessä on lista palveluntarjoajan palvelupyynnöistä (Ks. liite 2), jota käytettiin osana riskilistojen tekemisestä.

4.1.1 Resurssit

Ennen riskien kartoittamista arvioin yrityksen resursseja, joihin IT vaikuttaa. Resursseille pyrittiin antamaan selkeä arvo euroissa, jotta riskin vakavuutta voidaan arvioida myös kuluna.

Yrityksen toimiala on erityisen henkilöstöpainotteinen ja konsulttien työpanos yrityksessä lasketaan niin sanotun päivähinnan mukaan. Riskienhallinnan laskelmassa konsultin päivähinnaksi on määritelty 2000€. Päivähinnan kautta pystytään määrittelemään esimerkiksi yhden konsulttitunnin hinta tai koko yrityksen toiminnan seisahtamisen hinta kertomalla päivähinta konsulttien määrällä.

Yrityksellä on käytössä vähän laitteita ja käytännössä laitteista vain kannettavat tietokoneet ja puhelimet ovat merkittäviä kulueriä. Yhden koneen hinnaksi määriteltiin 1000 euroa asennustöineen ja puhelimen kuluksi 500 euroa. Verkkolaitteet ja palomuurit määriteltiin 2000€ arvoisiksi kappaleelta.

Yrityksellä on käytössään vain vähäisesti paikallisia tietojärjestelmiä, joista mikään ei ole liiketoimintakriittinen ja siten pääsy kyseisiin järjestelmiin tai järjestelmien heikko toimivuus ei juuri vaikuta liiketoimintaan. Lähinnä IT-henkilöstön käyttämä aika ongelmien korjaamiseen voidaan tulkita kuluksi kyseisten järjestelmien ongelmatilanteissa.

Yritykselle maine on erityisen tärkeä ja maineen menetystä voidaan pitää katastrofaalisena. Pelkästään vähäiset haitat maineeseen arvioidaan vakavuudeltaan merkittäviksi.

Yrityksellä on useita toimipisteitä eikä liiketoiminta ole sijainnista tai toimipisteestä riippuvainen. Yritys toimii vuokratiloissa eikä se omista omia toimitiloja. Kaikki yrityksen toimipisteet sijaitsevat paikoissa, joissa sähkö, vesi, tietoliikenne ja liikenneyhteydet ovat toimivia.

Muita resursseja pyrin arvioimaan tilannekohtaisesti. Esimerkiksi palvelun- tai tavarantoimittajia ja heidän aiheuttamien riskien mahdollisia menetyksiä ei tässä työssä lähdetty erikseen arvioimaan vaan vaikutukset pyrittiin arvioimaan henkilöstön menettämän työajan tai ylimääräisen aiheutuneen työn kautta.

4.1.2 Riskilistat

Riskilistojen laadinnan aloitin selvittämällä kaikki yrityksessä toteutuneet riskit, siltä ajalta, jonka olen työskennellyt yrityksessä. Selvitys oli hyvin muistinvarainen, koska suuresta osasta tapahtumia ei ole mitään dokumentaatiota. Selvitys ei sisältänyt kovin tarkkoja kuvauksia tapahtumista. Suuri osa riskeistä oli yleisiä, kuten hajonneita koneita ja kadonneita tiedostoja. Koin listauksen hyvin vajaaksi ja päädyin keskittymään tarkastelussa ulkoisiin lähteisiin.

Hain ulkoisista lähteistä tietoa mahdollisista riskeistä ja niiden syistä. Tässä yhteydessä Saksan tietoturvaviraston IT-Grundschutz-Catalogues osoittautui erinomaiseksi lähteeksi. Kyseinen dokumentaatio on yleisesti kaikkien käytettävissä ja dokumentaatio pitää sisällään noin 1300 erilaista IT-riskiä ja niiden kuvaukset sekä esimerkit.

Vuoden 2014 toukokuussa tehtiin yrityksen henkilöstölle tietohallinnon kysely, jossa selvitettiin normaalien toimintaan ja palveluihin liittyvien kysymysten lisäksi heidän mielipiteitään yrityksen IT-riskeistä. (Ks. liite 3). Kysymykseen vastasi 9 vastaajaa ja suuri osa vastauksista liittyi puhelinten suojaukseen. Kyselyn tuloksilla ei juuri ollut vaikutusta riskilistojen laatimiseen, koska kaikki mainitut mahdolliset riskit oli jo huomioitu.

Alustavassa riskilistassa määriteltiin vain riskin nimi ja jokainen riski arvioitiin siltä osin kohdistuuko kyseinen riski yrityksen paikallisiin IT-resursseihin. Riskit, joihin yrityksessä ei ole paikallisesti vaikuttamismahdollisuuksia, rajattiin suoraan pois tästä tutkimuksesta tai ne määriteltiin palveluntarjoajan toiminnaksi. Selvityksen tuloksena olivat riskilistat (Ks. liite 4).

4.1.3 Riskien analysoinnin toteutus

Kun riskit on tunnistettu, Suomisen mukaan päästään arvioimaan niiden laajuutta ja seurausvaikutuksia. Arviointityön avulla riskit pitää saada johonkin keskinäiseen järjestykseen. (Suominen 2003, 43)

Käytännössä riskien arviointi eteni siten, että riskejä tarkasteltiin riskilajeittain ja kunkin yksittäisen riskin todennäköisyys ja seurausvaikutukset arvioitiin suhteellisen karkealla asteikolla. Arvioin riskejä kolmessa vaiheessa teorian mukaisesti. Ensiksi pyrin määrittelemään sen resurssin arvon, johon riski vaikuttaa. Tämän jälkeen arvioin riskin vakavuus sen perusteella mihin resurssiin se vaikuttaa ja millä tavalla. Viimeisenä vaiheena arvioin riskin todennäköisyyden.

Käytin arvioinnissa määrällistä metodia (Ks. ed. s. 13), koska pidin sitä tilanteessamme luotettavampana. Yrityksellä ei ollut mielestäni riittävästi tietoa ja kokemusta, jotta laadullisen metodin käytöstä olisi saatu riittävän luotettava ja kattava. Kehittämistehtävässä käytin taulukon 3 mukaista luokittelua riskien vakavuuden arviointiin. Euromäärät pyrin sopeuttamaan yrityksemme kokoon ja liikevaihtoon.

Taulukko 3. Riskien vakavuus. (Suominen 2003, 44)

Riskien vakavuus	
1 Vähäinen riski	alle 200€
2 Kohtalainen riski	noin 1000€
3 Suuri riski	noin 5000€
4 Huomattava riski	noin 20000€
5 Katastrofiriski	vähintään 200000€

Lisäksi käytin Vahdin julkaisemia riskien vakaavuutta kuvaavia määritelmiä. Vahdin vakavuuden arvioinnissa on huomioitu eurojen sijaan toiminnallisia vaikutuksia ja se sopii osan riskeistä arviointiin siten paremmin.

Taulukko 4. Riskien vakavuus. (Vahti 2003, 25)

1 Vähäinen riski	Seuraukset koskevat muutamia tietojen tai palveluiden käyttäjiä
3 Suuri riski	Seurauksilla on vaikutuksia organisaation sisällä Seuraukset koskevat useita tietojen tai palveluiden käyttäjiä Seurauksilla on vaikutus organisaation toimintaan (saatava kuntoon tunneissa) Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia
5 Katastrofiriski	Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia Uhkan toteutuminen aiheuttaa vakavan häiriön organisaation toiminnassa (useiden avainhenkilöiden menetys) Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen

Riskien todennäköisyyttä varten muokkasin taulukon siten, että se soveltuu mielestäni aikaväleiltään paremmin yrityksemme käyttöön, kuin vastaavat kirjallisuuden tarjoamat vaihtoehdot.

Taulukko 5. Riskien todennäköisyys.

Riskien todennäköisyys	
1 äärimmäisen harvinainen riski	1 Kerta / yli 50 vuotta
2 harvinainen riski	1 Kerta /10-50 vuotta
3 melko harvinainen riski	1 Kerta / 5-10 vuotta
4 melko todennäköinen riski	Kerran vuodessa
5 erittäin todennäköinen riski	Kerran kuukaudessa

Pyrin valitsemaan käytetyt arviointiasteet sen perusteella, miten niistä saadaan helposti käyttökelpoisia vertailutietoja. Tässä kehittämistehtävässä käytin ainoastaan yksinkertaisia ja kirjallisuudessa käytettyjä asteikkoja. Monimutkaista laskentaa en halunnut

käyttää osittain välttääkseni mahdolliset virheet ja minimoidakseni siten virheiden vaikutukset päätöksentekoon, kun riskejä käsitellään. Kokeiltuani erilaisia asteikkoja ja useiden erilaisten kertoimien käyttämistä päädyin käyttämään valittuja 5 portaan asteikkoja. Riskit arvioitiin hyvin yleisellä tasolla riskilistavaiheessa ja niitä arvioitiin tarkemmin vasta siinä vaiheessa, kun niistä tehtiin riskienhallintasuunnitelma.

Jotta riskejä voidaan vertailla keskenään, kaikille riskeille laskettiin riskiarvo kertomalla riskin vakavuuden arvo riskin todennäköisyyden arvolla. Riskiarvo on hyvin karkea tapa ilmaista riskin kokonaisvakavuus mutta tässä kehittämistehtävässä arvioin tämän tasoisen arvioinnin riittäväksi. Riskiarvoa auttaa luokittelemaan tässä työssä riskit jonkinlaiseen järjestykseen ja sen avulla pystyn priorisoimaan riskienhallintasuunnitelmien tekemisen.

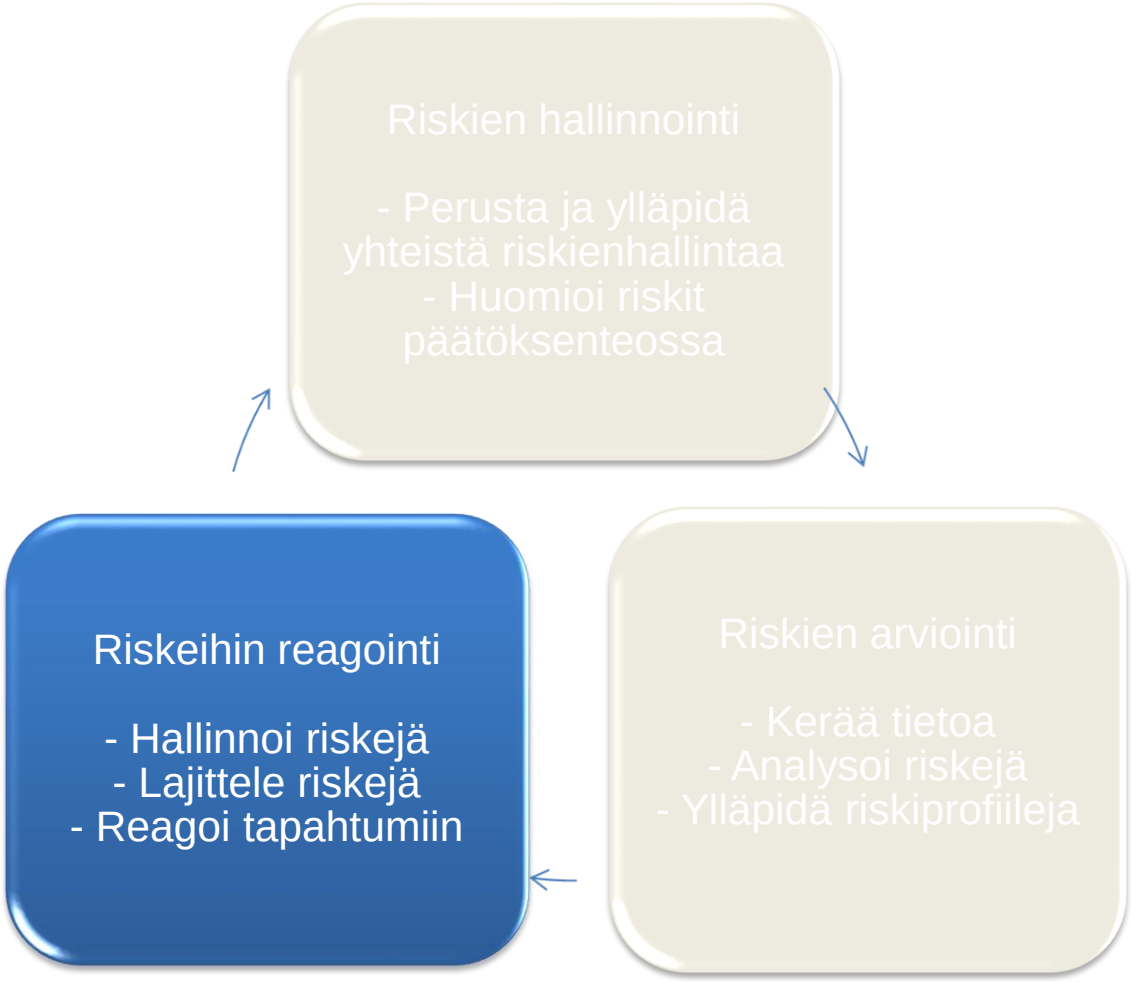
Tein riskiarvoille taulukon 6, jotta niitä voidaan myös pelkän lukuarvon sijaan ryhmitellä ja näin käsitellä selkeämmin. Päätin käyttää 5 tasoista taulukkoa todettuani, että riskejä on suuri määrä ja esimerkiksi kolmen tasoinen ryhmittely, jota useat lähteet ehdottivat, olisi mahdollisesti antanut vääränlaisen kuvan riskien kokonaisvakavuudesta.

Taulukko 6. Riskiarvot.

Riskiarvo	Riskin kokonaisvakavuus
21-25	Kriittinen
16-20	Vakava
11-15	Kohtalainen
6-10	Vähäinen
1-5	Merkityksetön

4.2 Riskeihin reagoinnin toteutus

Kuviossa 7 korostettuna COBIT:ssa määritelty riskeihin reagointiprosessi ja sen osat.



Kuvio 7. Riskeihin reagointiprosessi. (ISACA 2009, 15)

Yhtenä kehittämistyön tavoitteena on, että toteutuneista tapahtumista raportoidaan johdolle jatkossa säännöllisesti. Johtoryhmälle on tarkoitus raportoida vähintään kerran vuodessa laajemmin ja henkilöstölle suppeasti kuukausi-infon yhteydessä tai yleisellä viestillä. Raportoinnissa käydään läpi toteutuneet riskit ja niiden vakavuus sekä arvioidaan niiden vaikutuksia yrityksen toimintaan. Tietohallinnolla on vastuu raportoinnista ja pyrkimyksenä on lisätä ymmärrystä ja luoda läpinäkyvyyttä toteutuneisiin riskeihin sekä toimenpiteisiin.

Jatkossa tavoitteena on, että esimerkiksi budjetointiin ja kehittämissuunnitelmiin liittyviä päätöksiä voidaan suunnitella riskienhallinnan avulla. Tällöin saamme selkeää tietoa siitä minkälaisiin ja kuinka vakaviin riskeihin päätökset vaikuttavat.

4.2.1 IT-riskienhallintasuunnitelmien laatiminen

Seuraavassa vaiheessa aloin luoda riskienhallintasuunnitelmia. Riskienhallintasuunnitelmat on pyritty laatimaan siten, että riskin vakavuus on ollut tärkein prioriteetti, ja seuraavaksi on tullut se, onko riskiin olemassa mitään suunnitelmaa. Niissä riskeissä, missä jo jonkinlainen suunnitelma on ollut, on tietoisesti jätetty tekemättä uudenlainen lomakepohjainen varautumissuunnitelma kunnes vähintään vakavat ja kohtalaiset riskit on käyty läpi. Riskilistaa siis käytetään lähinnä riskisuunnitelmien tekemisen priorisoinnissa.

Riskienhallintasuunnitelmia varten luotiin lomake (Ks. liite 5). Jokainen riski kirjataan omalle lomakkeelleen. Taulukossa 7 ovat kuvaukset lomakkeen kentistä.

Taulukko 7. IT-riskienhallintasuunnitelmalomakkeen kentät.

Riskin nimi	Selkeä kuvaava nimi riskille.
Riskipisteytys	Riskin vakavuus ja todennäköisyys luku-arvona sekä näiden kerrottu riskiarvo.
Riskin lähde	Mistä riski saa todennäköisimmin alkunsa toteutuessaan. Lähde voi olla vaikka ihminen tai laite.
Riskin toteutuminen	Kuvaus mitä tapahtuu jos riski toteutuu.
Häiriintyneet toiminnot	Lista ja kuvaukset toiminnoista, joihin riski toteutuessaan vaikuttaa.
Varautuminen ja korjaavat toimenpiteet	Kuvaus miten riskeihin on varauduttu esimerkiksi vähentämällä riskiä tai siirtämällä sitä. Lisäksi kuvaus toimenpiteistä mitä on tarpeen tehdä jos riski toteutuu.
Vastuuhenkilöt	Lista henkilöistä, jotka ovat vastuussa kyseisestä riskistä ja sen torjumisesta.
Resurssit	Resurssit, joihin riski vaikuttaa.

4.2.2 Riskien ryhmittely

Riskien ryhmittelyyn löytyi monia hyviä keinoja, mutta lopulta päädyin tässä kehittämistehtävässä luokittelemaan riskit käytännön syistä samalla tavalla, kuin Saksan tietoturvaviraston IT-Grundschutz-Catalogues on sen tehnyt.

Saksan tietoturvaviraston dokumentaation ryhmittely on selkeä ja siinä luokitellaan riskit seuraaviin taulukon 8 mukaisiin ryhmiin.

Taulukko 8. Riskiryhmät. (Federal Office for Information Security, 2013. 418-1141)

Poikkeukselliset tapahtumat	Poikkeuksellisista olosuhteista johtuvia riskejä, kuten tulipalot, tulvat ja myrskyt
Organisaatiosta johtuvat IT-riskit	Organisaatioon ja sen toimintaan liittyvät IT-riskit, kuten käyttäjien heikko koulutus tai tiedonsaannin häiriöt
Ihmisistä johtuvat IT-riskit	Ihmisiin liittyvät riskit, kuten virheellinen ohjelmien käyttö ja tiedon syöttäminen väärin järjestelmiin.
Tahallisesti aiheutetut riskit	IT-riskit, joita voidaan pitää tahallaan aiheutettuina, kuten hyökkäykset yrityksen verkkoa vastaan tai tietojenkalasteluyritykset
Tekniset IT-riskit	Tekniikkaan liittyvät IT-riskit, kuten laitteiden hajoaminen

Tässä kehittämistehtävässä käytin vain yhtä ryhmittelyä, koska ajallisesti useamman ryhmittelyn tekeminen olisi vienyt liikaa aikaa ja saatu hyöty ei välttämättä olisi ollut riittävä.

4.2.3 Jatkuvan seurannan rakentaminen

Jatkuvaa seurantaa varten loin taulukon, jolla tarkastetaan toteutuneita riskejä verrattuna suunnitelmiin (Ks. liite 6). Kerran vuodessa suoritan arvioinnin mahdollisista uusista riskeistä jos se nähdään tarpeelliseksi huomioiden muuttuneet resurssit, toteutuneet riskit ja muuttunut liiketoimintaympäristö.

Jokainen havaittu turvallisuustapahtuma kirjataan tietohallinnon toimesta ja listaa verrataan tiedostettujen IT-riskien listaan. Jos havaittua riskiä ei ole aikaisemmin todettu, kyseinen riski lisätään riskilistaan ja sille luodaan oma riskilomake.

4.3 Viestintä ja muutosjohtaminen

Esittelin projektin johtoryhmän kokouksessa maaliskuussa 2014. Kerroin kehittämistehtävän toteutustavasta ja perustelin aiheen valintaa. Henkilöstölle projektista ilmoitettiin saman kuukauden kuukausi-infossa, jossa projekti esiteltiin lyhyesti. Tässä yhteydessä ilmoitin myös vuosittaisesta tietohallinnon kyselystä. Tietohallinnon kyselyssä selvitettiin henkilöstön näkemyksiä yrityksen IT-riskeistä yhdellä kysymyksellä ja annettiin henkilöstölle mahdollisuus tuoda omia näkemyksiään aiheesta esille.

Lokakuussa 2015 esittelin työn tuloksia johtoryhmän kokouksessa. Pyrin kehittämistehtävän aikana säännöllisesti keskustelemaan esimieheni ja johtoryhmän jäsenten kanssa projektin etenemisestä. Johdon kanssa käymilläni keskusteluilla pyrin vaikuttamaan siihen, kuinka tärkeänä kehittämistehtävä nähdään yritykselle ja sitä kautta kuinka paljon aikaa pystyin käyttämään sen tekemiseen. Olen kaikissa mahdollisissa tilanteissa pyrkinyt lisäämään tietoisuutta yritykseen kohdistuvista uhkista ja riskeistä. Sivulla x kuvatussa Muutoksen portaissa on hyvin määritelty tapoja johtaa muutosta. Olen pyrkinyt olemaan tietoinen kaikista mahdollisista muutoksista, joita yrityksessä tapahtuu tai saattaa tapahtua. Tällä tavoin on ollut helpompi toimia tietohallinnon tehtävissä ja helpompi reagoida mahdollisiin muutoksiin.

Kehittämistehtävä vei paljon aikaa ja välillä työn aikana kyseenalaistin, onko tämänlainen riskienhallinta todella tarpeellinen yrityksessämme, ja kuinka paljon voin käyttää tähän aikaa. Vaikka minun ei tarvinnut vaikuttaa merkittävästi yrityksen henkilöstöön tämän kehittämistehtävän aikana, olen kuitenkin pyrkinyt omassa asennoitumisessani ja motivaation ylläpitämisessä siihen, että epäilykseni työstä ja sen vaikutuksista ei hidastanut työn valmistumista. Itsensä motivointi onkin ollut työssä oleellisin keino muutoksen johtamisessa.

Kehittämistehtävän tarkoituksena on saada mitattavia tuloksia muutoksesta. Muutoksen mittaaminen on oleellinen osa muutoksen johtamista, ja tässä kehittämistehtävässä muutokselle määriteltiin riittävästi mittareita. Olen pyrkinyt välttämään ylimittaamista

tietoisesti, jotta tuloksista saadaan tässä vaiheessa riittävän yksinkertainen ja tuloksena kehittämistehtävästä selkeä näkymä yrityksen tilanteeseen.

Pyrin kehittämistehtävän aikana herättämään keskustelua käyttäjien kanssa ja yritin saada heidät ajattelemaan yritykseemme kohdistuneita riskejä ja siten osallistumaan riskien määrittelyyn esimerkiksi kyselyyn lisätyllä kysymyksellä. Tämä herättikin jonkin verran ajatuksia vaikka ei itsessään vaikuttanutkaan työn kulkuun tai sen tuloksiin. Alkutiedotusta ja kyselyä lukuun ottamatta en kokenut tarpeelliseksi järjestää erillistä koulutusta tai tilaisuutta IT-riskeistä tässä vaiheessa.

Mielestäni teorian oleellisimpia kohtia muutosjohtamisen kannalta on se, että opin tuntemaan ihmiset ja annan heidän tutustua itseeni, jos he sitä haluavat. Olen koko yrityksessä työskentelyn ajan pyrkinyt olemaan tavoitettavissa ja läsnä toimistolla, vaikka minulla onkin erillinen työhuone. Lisäksi käyn usein Turun ja Oulun toimistoillamme ja vietän siellä enemmän aikaa, kuin työtehtävät vaatisivat. Tarvittaessa henkilöstö voi myös näissä toimistoissa saada tilaisuuden keskustella kanssani ja mahdollisesti kertoa pienemmistä ongelmista tai parannusehdotuksista, joita ei muuten välttämättä jaettaisi. On huomattavasti helpompi vaikuttaa ihmisiin ja saada heidät kuuntelemaan, kun heillä on käsitys omista näkemyksistäni ja tavoitteistani. Saan myös enemmän tietoa käyttäjien ongelmista ja yritykseen kohdistuvista riskeistä ja niiden toteutumisesta, kun ihmiset tuntevat minut ja voivat tarvittaessa tulla puhumaan kanssani ongelmista.

5 Kehittämistehtävän tulokset

Tässä kappaleessa käsittelen tuloksia tutkimuskysymysten ja niihin liittyvien mittarien kautta. Taulukossa 9 ovat tutkimuskysymyksiin liitetyt mittarit.

Taulukko 9. Tutkimuskysymyksiin liitetyt mittarit.

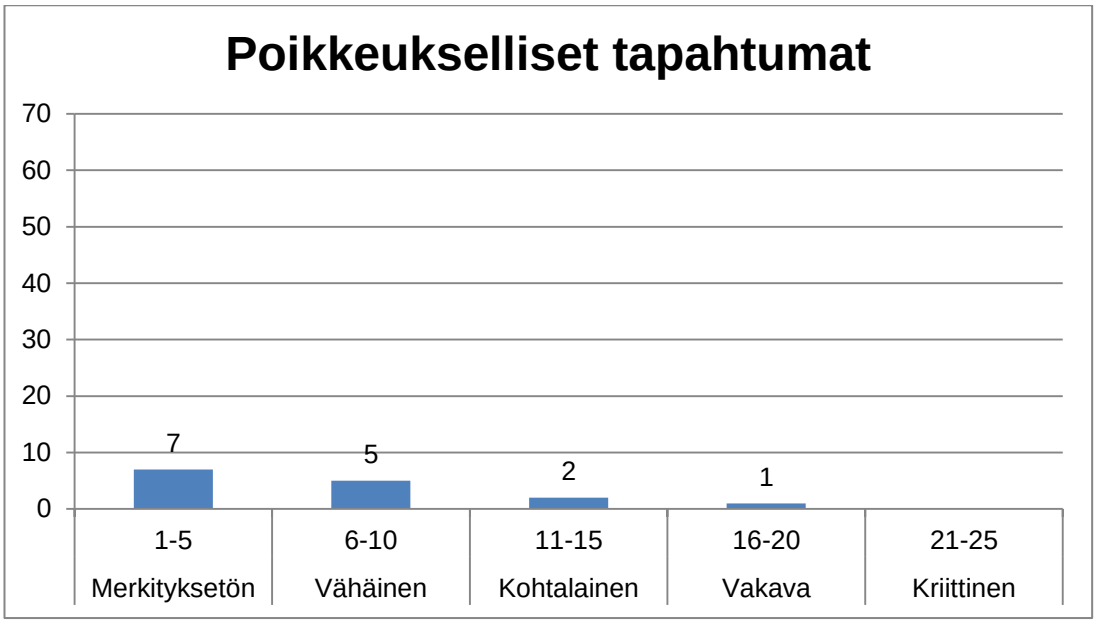
Tutkimuskysymys	Mittari
Kuinka paljon ja kuinka vakavia riskejä havaitaan tekemällä riskikartoitus?	Todettujen riskien määrä ja niiden riskiarvot.
Kuinka paljon suunnitelmallinen riskienhallinta lisää suunnitelmien ja ohjeistusten määrää yrityksessä?	Kriittisten ja vakavien IT-riskien määrä, joita varten on tehty riskienhallintasuunnitelma verrattuna suunnittelemattomaan lähtötilanteeseen.
Minkälaisia ja kuinka vakavia riskejä, joihin ei yrityksessä ole varauduttu, löydetään siirryttäessä suunnitelmalliseen riskienhallintaan?	Riskien, joihin ei ole varauduttu, määrä ja riskiarvot.
Kuinka paljon riskejä löytyy jatkuvan seurannan avulla, joita ei ole aikaisemmin havaittu?	Uusien riskien määrä, jotka todetaan säännöllisessä riskien tarkastelussa ja niiden merkittävien tapahtumien määrä, jotka aiheutuivat tunnistamattomasta IT-riskistä.

5.1 Riskien määrä ja riskiarvot

Kysymykseen, kuinka paljon ja kuinka vakavia riskejä havaitaan tekemällä IT-riskien kartoitus, pyrittiin vastaamaan käyttämällä mittareina todettujen riskien määrää ja niiden riskiarvoja.

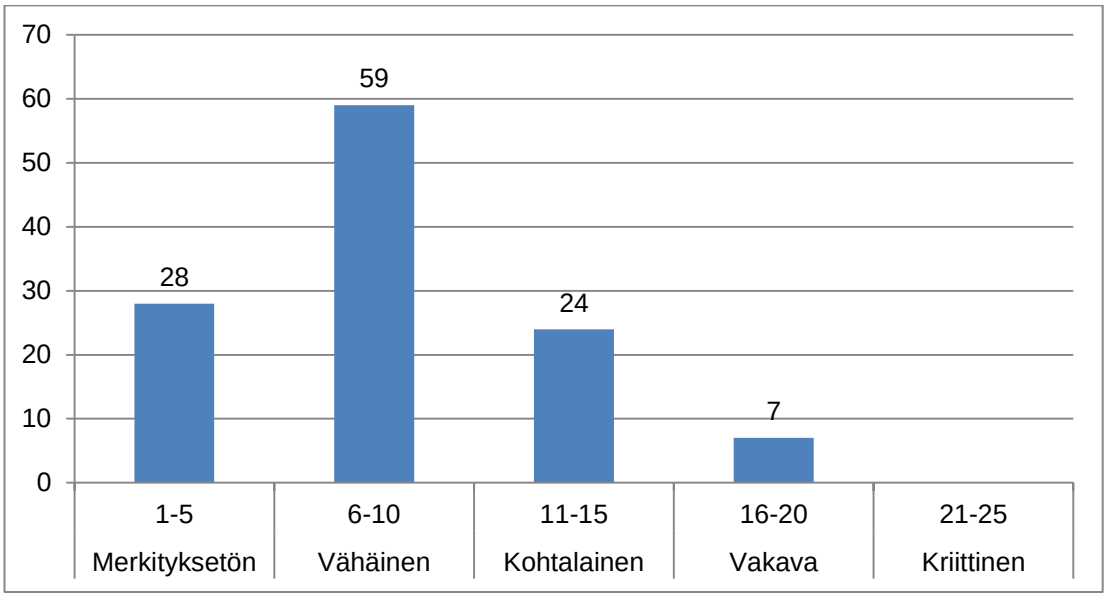
Riskikartoituksessa riskejä todettiin yhteensä 293 kappaletta. Riskit käsiteltiin myös ryhmittäin, jotta niistä pystytään raportoimaan johdolle selkeämmin ja samalla voidaan helpottaa riskien torjuntaan käytettävien resurssien jakamista tulevaisuudessa.

Poikkeuksellisiin tapahtumiin luokiteltiin yhteensä 15 riskiä. Riskit jakautuivat kuvion 8 mukaisesti.



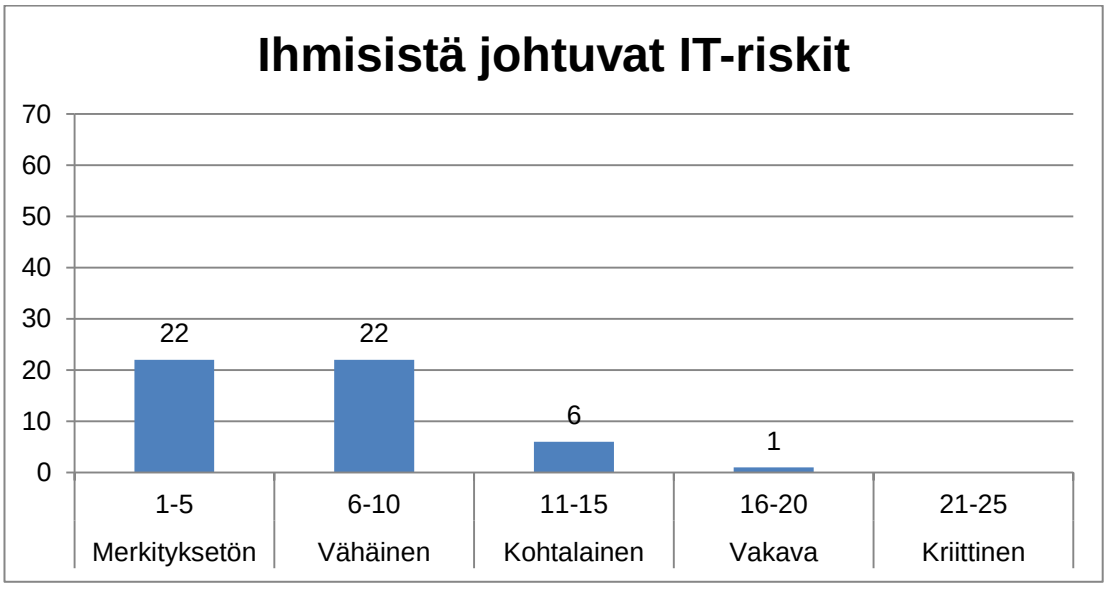
Kuvio 8. Poikkeukselliset tapahtumat.

Organisaatioon ja sen toimintaan liittyviä IT-riskejä todettiin 88 kappaletta.



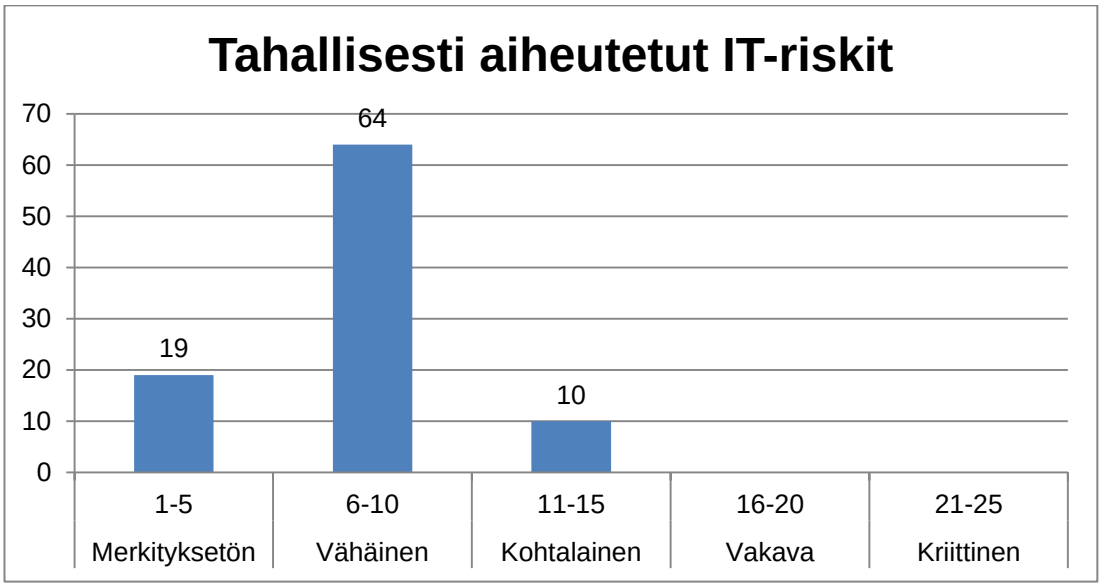
Kuvio 9. Organisaatiosta johtuvat IT-riskit.

Ihmisistä johtuvia IT-riskejä todettiin 51 kappaletta.



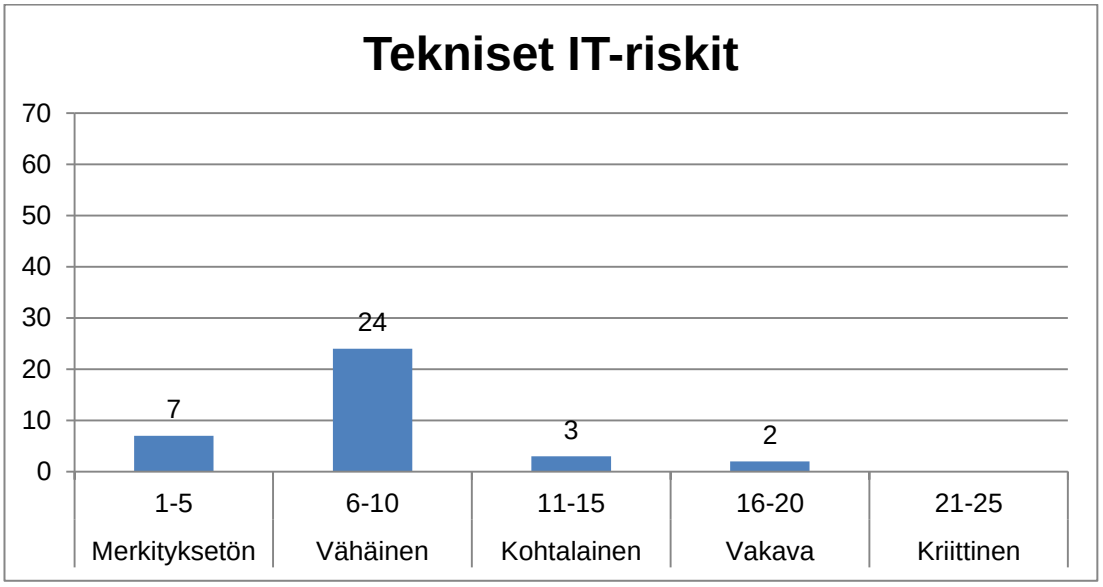
Kuvio 10. Ihmisistä johtuvat IT-riskejä.

Tahallisiksi IT-riskeiksi luokiteltuja riskejä todettiin 93 kappaletta.



Kuvio 11. Tahalliset riskit.

Teknisiä IT-riskejä todettiin 36 kappaletta.



Kuvio 12. Tekniset IT-riskit.

Määrällisesti merkittävin ryhmä oli organisaatiosta johtuvat riskit. Samoin vakavia riskejä löytyi eniten organisaation liittyvistä riskeistä. Tuloksien perusteella yrityksen onkin

hyvä panostaa oman toimintansa tarkasteluun ja priorisoida riskeihin varautumisen suunnittelu organisaatioon liittyviin riskeihin

5.2 Riskeihin varautuminen

Toisena tutkimuskysymyksenä oli minkälaisia ja kuinka vakavia riskejä, joihin ei yrityksessä ole varauduttu, löydetään siirryttäessä suunnitelmalliseen riskienhallintaan. Kysymykseen pyrittiin vastaamaan käyttämällä alkutilanteessa riskien määrää, joihin on varauduttu, ja vertaamalla lukuja todettujen riskien määriin ja niiden riskiarvoihin. Alkutilanne ohjeiden ja varautumissuunnitelmien suhteen oli taulukon 10 mukainen.

Taulukko 10. Lähtötilanne.

Alkutilanne			
Riskin kokonaisvakavuus	**Riskiarvo**	**Todettujen riskien määrä**	**Riskien määrä, joihin varauduttu**
Kriittinen	**21-25**	**0**	**0**
Vakava	**16-20**	**14**	**7**
Kohtalainen	**11-15**	**57**	**25**
Vähäinen	**6-10**	**197**	**53**
Merkityksetön	**1-5**	**74**	**9**

Riskejä, joihin yrityksessä ei löytynyt suunnitelmia, oli yhteensä 248. Voidaan todeta, että yrityksessä ei ollut varauduttu riskeihin kovin hyvin. Vakavissa riskeissä oli suunnitelmia puoleen riskeistä, kohtalaisissa, vähäisissä ja merkityksettömissä riskeissä reilusti alle puolet. Tulosta voidaan pitää huonona yrityksen kannalta. Aikaisemmin riskienhallinta on ollut liiaksi arvionvaraista ja siten riskien toteutumisesta aiheutuneita haittoja on voinut olla merkittävästi. Toisaalta hyvänä voidaan pitää sitä, että riskikartoituksessa havaittiin paljon uusia riskejä ja niihin voidaan jatkossa varautua suunnitelmallisemmin.

5.3 Riskienhallintasuunnitelmat

Seuraavana tarkasteltiin tutkimuskysymystä kuinka paljon suunnitelmallinen riskienhallinta lisää suunnitelmien ja ohjeistusten määrää yrityksessä. Tähän pyrittiin vastaamaan määrittelemällä niiden kriittisten ja vakavien IT-riskien määrä, joita varten on tehty riskienhallintasuunnitelma verrattuna suunnittelemattomaan lähtötilanteeseen.

28.8.2015 tarkastettu tilanne oli taulukon 11 mukainen. Tarkastelussa laskettiin yhteen uudet ja vanhat riskienhallintasuunnitelmat ja ohjeistukset.

Taulukko 11. Tilanne 28.8.2015.

Tilanne 28.8.2015			
Riskin kokonaisvakavuus	Riskiarvo	Todettujen riskien määrä	Riskien määrä, joihin varauduttu
Kriittinen	21-25	0	0
Vakava	16-20	14	14
Kohtalainen	11-15	57	35
Vähäinen	6-10	197	53
Merkityksetön	1-5	74	9

Voidaan todeta, että kaikki vakavaksi todetut riskit on pystytty kattamaan joko uusilla tai vanhoilla suunnitelmilla. Kohtalaisiksi todetuista riskeistä on varauduttu kymmeneen riskiin enemmän alkutilanteeseen verrattuna. Muissa riskiluokissa ei muutosta ole tapahtunut.

Työn tavoitteena oli saada kaikkiin kriittisiin ja vakaviin riskeihin riskienhallintasuunnitelmat. Tuloksia voidaan pitää hyvinä, koska tämä tavoite saavutettiin. Riskienhallintasuunnitelmien tekeminen on hidasta ja siitä syystä kaikkiin kohtalaisiin riskeihin ei arviointihetkellä ollut varauduttu.

5.4 Jatkuva seuranta

Tutkimuskysymykseen, kuinka paljon riskejä löytyy jatkuvan seurannan avulla, joita ei ole aikaisemmin havaittu, pyrittiin löytämään vastaus kahdella mittarilla. Mittareina toimivat uusien riskien määrä, jotka todetaan säännöllisessä riskien tarkastelussa ja niiden merkittävien tapahtumien määrä, jotka aiheutuivat tunnistamattomasta IT-riskistä.

Toteutuneiden riskien tarkastelu tehtiin elokuun 2015 aikana ja tarkastelussa ei havaittu yhtäkään tunnistamatonta riskiä seurannan ajalta eikä tarvetta lisätä uusia riskejä riskilistaan ole. Jatkuvalla seurannalla on kerätty lista todetuista tapahtumista. (Ks. liite 6) Suurin osa on hajonneita laitteita, joista neljä kappaletta oli kannettavia tietokoneita ja puhelimia viisi kappaletta. Kaksi pitkään kestänyttä häiriötä puhelinliittymissä olivat vakavimmat todetuista riskeistä. Yksikään toteutunut riski ei ole sellainen, mitä ei ole aikaisemmin havaittu ja kirjattu riskilistaan. Tuloksena tämä on yrityksen kannalta erit-

täin hyvä. Kaikki havaitut riskit on pystytty määrittelemään etukäteen ja niille löytyi riskienhallintasuunnitelma. Puhelimien liittymiin liittyvissä ongelmissa oli tarve lisätä ja päivittää suunnitelmia, koska suunnitelmat olivat puutteellisia.

6 Yhteenveto ja johtopäätökset

Tässä kappaleessa käyn läpi ja arvioin työn tuloksia. Lisäksi käyn läpi mahdollisia jatkotoimenpiteitä. Kehittämistehtävällä pyrittiin parantamaan yrityksen riskienhallintaa ja tunnistamaan yritykseen ja sen liiketoimintaan kohdistuvia IT-riskejä. Tässä tavoitteessa mielestäni onnistuttiin, koska riskilistoista saatiin mielestäni hyvin kattavia ja riskeihin pystytään varautumaan jatkossa paremmin. Uskon, että työtä tullaan hyödyntämään yrityksessä jatkossa ja kehittämistehtävälle asetetut tavoitteet täyttyvät.

Todettujen riskien määrä oli yllättävän suuri ja alustava arvioni noin sadasta riskistä ylittyi reilusti. Lisäksi yllättävänä voidaan pitää sitä, että riskeihin löytyi hyvin vähän minkäänlaisia suunnitelmia tai ohjeistuksia, vaikka yrityksen tietohallinnon ohjeistus on kattava. Aikaisemmin siis suurin osa toteutuneisiin riskeihin reagoinnista on tapahtunut tilanteen mukaan ja toimenpiteet ovat siten varmasti olleet hitaampia.

Alkuun tehtyä riskienkartoitusta voidaan mielestäni pitää onnistuneena, koska puoleen vuoteen ei ole havaittu riskejä, joita ei ole tiedostettu tai joihin ei ole varauduttu. Voidaankin todeta, että riskilistat ovat kattavia ja pitävät sisällään laajasti mahdollisia riskejä. Todennäköisesti jatkossa havaitaan uusia riskejä ja oleellista onkin säännöllisesti arvioida mahdollisia uusia riskejä yritykselle. Riskianalyysejä tehdessä yhtäkään kriittistä riskiä ei todettu. Tätä voidaan pitää yrityksen kannalta hyvänä asiana.

Vaikka seuranta on hyvä asia, on seuranta toisaalta hankalaa, koska esimerkiksi käyttäjän virheistä ei aina tule tietoa tietohallinnolle. Tämä osaltaan selittää todettujen toteutuneiden riskien vähäistä määrää.

Pidän työtä osittain keskeneräisenä, koska iso osa riskisuunnitelmista on edelleen tekemättä. Toisaalta vähäisten riskien suunnitelmien teon olen jättänyt tietoisesti ajankäytön takia myöhemmäksi.

Kehittämistehtävän tavoitteena oli tuoda yrityksen IT-riskienhallinta sivulla 5 esitetyn kypsyysmallin tasolle 4 alkutilanteen tasosta 1. Tällä hetkellä tilanteemme on mielestäni hieman huonompi kuin tavoiteltu taso ja kypsyysmallin taso 3 on arvioni mukaan oikea. Yritykselle on määritelty prosessi IT-riskienhallintaa varten ja prosessissa on määritelty miten ja milloin riskienarviointi tehdään. Prosessi on myös tämän kehittämistehtävän myötä dokumentoitu. Kypsyysmallin tasosta 4 näkisin puuttuvan nykytilanteessamme kaikkien poikkeavuuksien raportoinnin puutteen, koska osaa riskeistä ei mielestäni riittävän hyvin pystytä todentamaan ja kaikkiin riskeihin ei vielä ole määritelty suunnitelmaa.

Muutoksen seuranta ja mittaaminen on erityisen tärkeää kehittämistehtävän onnistumisen kannalta. Jotta saadaan aikaan pysyvä muutos, on hyvä seurata minkälaisia vaikutuksia työllä on pidemmällä aikavälillä. Muutoksen johtamisen kannalta kehittämistehtävä on mielestäni onnistunut. Jatkossa voimme säännöllisellä seurannalla mitata kehittämistehtävän tuomia hyötyjä. Olen saanut käyttööni työkaluja, joilla johdolle voidaan perustella hankintoja ja näyttää arvioita vaikutuksista.

Alkuperäiseen suunnitelmaan kuului taloudellisia mittareita sekä tutkimusta riskienhallinnan vaikutuksista liiketoimintaan ja työntekijöihin, mutta nämä tavoitteet eivät tässä työssä täyttyneet. Vaatisi huomattavasti lisää työtä tehdä niin kattava tutkimus. Tämä ei kuitenkaan mielestäni vähennä saavutettujen tuloksien arvoa ja jatkossa tämä työ mahdollistaa myös jatkokehityksen vaativampaan selvittelyyn.

Viitekehyksen kaikki osa-alueet toimivat mielestäni hyvin työn ohessa. Osaa teoriasta ei voinut juurikaan hyödyntää, mutta suuri osa alkuperäisestä teoriasta osoittautui käyttökelpoiseksi. Muutosjohtamista olisin toivonut pääseväni käytännössä käyttämään ja tarkastelemaan enemmän, mutta työn rajauksen takia tällä työllä on vaikutusta lähinnä vain johtoon. Näin ollen vaikutusmahdollisuudet muuhun henkilöstöön jäivät vähäisiksi.

6.1 Viitekehyksen toimivuus kehittämistehtävässä

Kehittämistehtävän viitekehys oli mielestäni toimiva ja sain viitekehyksen mukaisesti toteutettua hyvin työn vaiheet. Muutamissa työvaiheissa jätin tietoisesti tekemättä toimenpiteitä teorian perusteella, koska ne olivat liian vaativia tai niiden tekeminen olisi vaatinut liikaa aikaa. Nämä kohdat on jätetty IT-riskienhallinnan jatkokehitystä varten.

Käytin vähäisesti eri teorialähteitä viitekehyksen rakentamisessa. Tarkoitukseni oli pyrkiä käyttämään mahdollisimman paljon COBIT:n tarjoamia keinoja ja suosituksia ja käytin siksi muuta teoriaa vain niissä vaiheissa, joihin COBIT ei tarjonnut riittävän tarkkoja suosituksia toimintaan.

6.2 Reliabiliteetti ja validiteetti

Hirsjärvi, Remes ja Sajavaara toteavat, että tutkimuksen reliaabelius tarkoittaa mittaustulosten toistettavuutta. Mittauksen tai tutkimuksen reliaabelius tarkoittaa siis sen kykyä antaa ei-sattumanvaraisia tuloksia. Reliaabelius voidaan todeta usealla tavalla. Esimerkiksi jos kaksi arvioijaa päätyy samaan tulokseen, voidaan tutkimusta pitää reliaabelina, tai jos samaa henkilöä tutkitaan eri tutkimuskerroilla ja saadaan sama tulos, voidaan jälleen todeta tulokset reliaabeleiksi. (Hirsjärvi & Remes & Sajavaara 2007, 226)

Tutkimus ja sen tulokset perustuvat suurelta osin riskiarvioihin, jotka ovat subjektiivisia arvioita riskien todennäköisyydestä ja vakavuudesta. Kaikki riskiarviot ovat omia arvioitani ja sitä kautta toisen henkilön tekemänä tulokset olisivat todennäköisesti erilaiset. Reliabiliteettia voitaisiin lisätä sillä, että joku muu, esimerkiksi ulkopuolinen taho, arvioisi riskit. Tässä työssä ulkopuolisia tahoja ei kuitenkaan arvioissa voitu käyttää ja yrityksen oman henkilöstön keskuudesta en arvioinut löytyvän riittävää näkemystä riskien todennäköisyyksien ja vakavuuksien arviointiin.

Toinen tutkimuksen arviointiin liittyvä käsite Hirsjärven ym. mukaan on validius. Validius tarkoittaa mittarin tai tutkimusmenetelmän kykyä mitata juuri sitä, mitä on tarkoituskin mitata. (Hirsjärvi ym. 2007, 226.)

Olen pyrkinyt valitsemaan käytetyt teoriat sen perusteella, että ne soveltuvat mahdollisimman hyvin yrityksen ongelman ratkaisuun. Olen pyrkinyt mahdollisimman tarkasti selostamaan tekemäni toimenpiteet ja käyttämäni teoriat. Lisäksi olen pyrkinyt perustelemaan miksi olen päätynyt tuloksiin, joita kehittämistehtävässä on ilmennyt. Kehittämistehtävässä asetettuihin kysymyksiin saatiin mielestäni vastaus. Tutkimus julkaistaan anonyyminä ja yrityksen tiedot ja osa tuloksista salataan. Tämän takia kaikki tieto kehittämistehtävän taustoista ja tuloksista ei selviä lukijalle.

6.3 Jatkokehitys

Kehitystehtävä jäi alkuperäisiin suunnitelmiin nähden keskeneräiseksi. Tavoitteena on jatkossa saada kaikille todetuille riskeille riskienhallintasuunnitelmat ja mahdollisesti laajentaa myös riskienhallintaa käsittämään kaikkia IT-riskejä pelkästään paikallisten IT-riskien sijaan. Tämä vaatisi huomattavaa määrää yhteistyötä kansainvälisen organisaation kanssa.

Jatkossa riskien arviointia voidaan pyrkiä muuttamaan nykyisestä karkeasta arviosta enemmän laskentaa sisältävään arviointiin. Tällöin huomioitaisiin tarkemmin riskeihin liittyvät kulut, resurssit ja esimerkiksi riskeihin varautumiseen käytetty työaika. Riskien ryhmittelyyn on tarvetta lisätä uusia tapoja. Luokittelemalla riskit useammalla kuin yhdellä tavalla saadaan päätöksentekoon lisää työkaluja ja voidaan suunnata resursseja oikeisiin asioihin.

Riskienhallinnan taloudelliset vaikutukset jäivät tässä työssä käsittelemättä. Jatkossa olisi hyvä selvittää kuinka erilaiset keinot varautua riskeihin vaikuttavat kuluihin ja käytetäänkö toisiin riskeihin liikaa tai liian vähän resursseja vakavuuteen nähden. Kun riskeihin varaudutaan, liittyy siihen usein koulutusta ja perehdytystä. Tarkoituksena on riskisuunnitelmien pohjalta suunnitella koulutusmateriaalia käyttäjille ja tarvittaessa kouluttaa pääkäyttäjiä ja IT-henkilöstöä.

Lähteet

Arikoski, Juha & Sallinen, Mikael 2007. Vastarinnasta vastarannalle – johda muutos taitavasti. Otavan Kirjapaino Oy, Keuruu.

Erola, Eero & Luoto, Pentti 2000. Riskit voimavaraksi – liiketoimintariskien hallinta yrityksessä. Oy Edita Ab, Helsinki.

Erämetsä, Timo 2003. Myönteinen muutos. Vammalan kirjapaino Oy, Sastamala.

Harris, Shon 2007. All in One CISSP Exam Guide. McGraw-Hill Osborne Media.

Heikkinen, Hannu L.T. & Rovio, Esa & Syrjälä, Leena 2007. Toiminnasta tietoon. Toimintatutkimuksen menetelmät ja lähestymistavat. Dark Oy, Vantaa.

Holstnider, Bill & Jaffe, Brian 2010. IT Manager's Handbook. Morgan Kaufmann Publishers, Burlington.

ISACA 2009. The Risk IT Framework. ISACA, IL.

ISACA 2012. COBIT 5 Enabling Process. ISACA, IL.

IT Governance Institute 2007. COBIT 4.1. IT Governance Institute, IL.

Federal Office for Information Security 2013. IT-Grundschutz-Catalogues 13t version 2013.
https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html. Luettu 25.10.2014

Jordan, Ernie & Silcock Luke 2006. Strateginen IT-riskien hallinta. Edit Publishing Oy, Helsinki.

Yritys X 2014a. Verkkosivut. Luettu 30.10.2015

Yritys X 2014b. Sisäinen tieto.

Suominen, Arto 2003. Riskienhallinta. Dark Oy, Vantaa.

Yrityksen visio, strategia ja tavoitteet

LUOTTAMUKSELLINEN

Palvelupyynnöt palveluntarjoajalle 1.1.2012-22.8.2015

LUOTTAMUKSELLINEN

Tietohallinnon kyselyn tulokset riskeistä

LUOTTAMUKSELLINEN

Riskilistat

LUOTTAMUKSELLINEN

Riskilomake

Riski			
Riskipisteytys	Todennäköisyys	Vakavuus	Riskipisteet
Toimenpiteet			
Riskin toteutuminen			
Häiriintyneet toiminnot			
Varautuminen ja korjaavat toimenpiteet			
Vastuuhenkilöt			
Resurssit			

Esimerkki: toteutuneet riskit

Toteutuneet riskit				
Riskin nimi	Päiväys	Resurssit	Arvioitu kustannus	Vakavuus
Hajonnut laite	20.1.2015	Kannettava tietokone	800 €	2
Hajonnut laite	6.3.2015	Kannettava tietokone	1 000 €	2
Hajonnut puhelin	9.3.2015	Puhelin	400 €	2
Hajonnut puhelin	26.3.2015	Puhelin	400 €	2
Hajonnut laite	1.5.2015	Kannettava tietokone	800 €	2
Puhelinyhteydet poikki 5h	5.5.2015	Koko henkilöstö	5 000 €	4
Vahingossa tuhottu tiedosto	5.5.2015	Yksi tiedosto	-	1
Hävinnyt laite	2.6.2015	Yksi kannettava tietokone	800 €	1
Varastettu laite		Puhelin	400 €	3
Puhelinyhteydet poikki 1h	6.8.2015	Koko henkilöstö	1 000 €	4
Viruksia koneella	10.8.2015	Kannettava tietokone	140 €	3
Hajonnut puhelin	13.8.2015	Puhelin	400 €	2
Hajonnut puhelin	20.8.2015	Puhelin	400 €	2
Kadonnut tiedostokansio	20.8.2015	Tiedostokansio	140 €	1
Hajonnut puhelin	25.8.2015	Puhelin	400 €	2